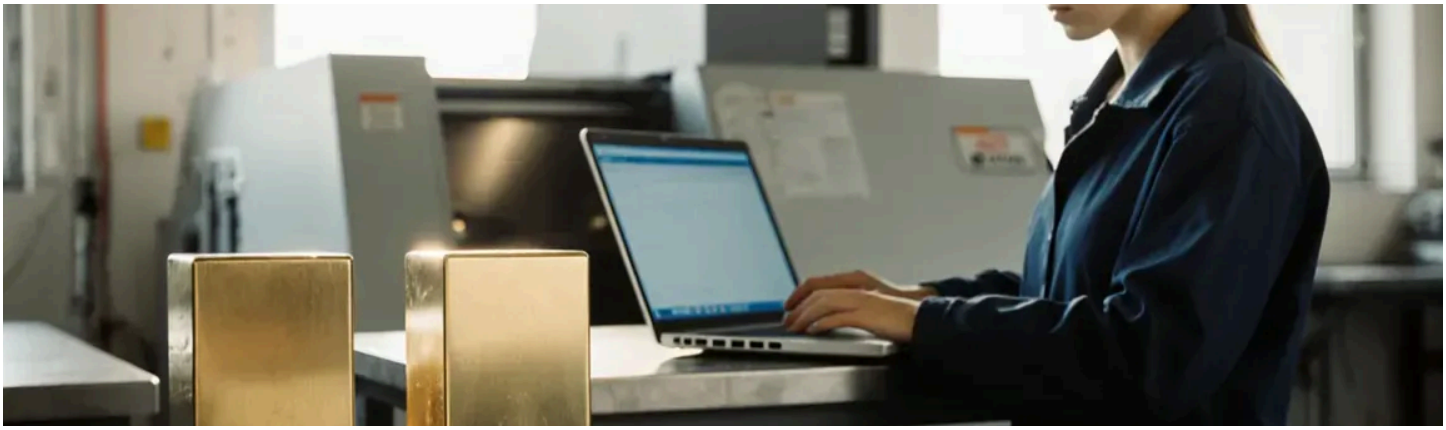


CMMC Phase II Is Paused. Your 800-171 Obligations Are Not.

November 10, 2026 was supposed to be the day third party CMMC certification became a condition of award for many defense contracts. It came and went without that requirement, and some suppliers are treating the pause as permission to stop spending on security and CMMC compliance.

Dave Hoon
Chief Technology Officer, Norseman Defense Technologies · November 2026

November 10, 2026 was supposed to be the day third party CMMC certification became a condition of award for many defense contracts. It came and went without that requirement, and some suppliers are treating the pause as permission to stop spending on security and CMMC compliance.

That is a costly misreading. The pause changed how the Department of War (DoW) plans to verify cybersecurity. It did not change what defense suppliers must actually do.

What Changed in 2026

Phase II was suspended. On July 13, 2026, DoW announced the immediate suspension of CMMC Phase II. Phase II would have required contractors handling Controlled Unclassified Information (CUI) to obtain Level 2 certification from a Certified Third Party Assessment Organization (C3PAO). The memo, signed by DoW Chief Information Officer Kirsten Davies, also put Phases III and IV on hold and created a CMMC Reform Task Force to carry out a 60 day review. DoW said "all Phase 1 self-assessment requirements remain firmly in place."

The pause became binding on contracting officers. A DoW class deviation dated September 3, 2026 (DFARS class deviation 2026-O0025, Revision 3) directs contracting officers to remove third party CMMC requirements from

solicitations and contracts. According to published legal analyses, it also requires baseline compliance with NIST SP 800-171 Revision 2 under DFARS 252.204-7012.

Industry weighed in, and the cost driver is the controls themselves. DoW's request for information closed August 14, 2026. Federal News Network reported on October 26, 2026 that the task force reviewed 997 qualifying comments, and that respondents' top cost driver was "meeting the security control requirements" of NIST SP 800-171, not the CMMC program itself.

A restart is on the table. Federal News Network reported on October 27, 2026 that the task force's options include restarting Phase II "with a narrower population" within 90 days, finalizing the move to NIST SP 800-171 Revision 3, and extending the time allowed to close open items. None of these has been approved. As of early November 2026, DoW had not published the task force report or a new Phase II date.

What Remains in Force Today

Law firms that advise defense contractors agree on the basics:

- **DFARS 252.204-7012** still requires adequate security for covered defense information, based on NIST SP 800-171, plus rapid cyber incident reporting.
- **DFARS 252.204-7019 and 7020** still tie awards to a current NIST SP 800-171 assessment score posted in the Supplier Performance Risk System (SPRS).
- **CMMC Phase I** self assessments for Level 1 and Level 2 remain in effect where contracts require them.
- **FAR 52.204-21** basic safeguarding still applies to Federal Contract Information.
- **False Claims Act exposure** remains. As Morgan Lewis noted, the Department of Justice's Civil Cyber-Fraud Initiative is "unaffected by the suspension."

In plain terms: the pause removed one way of checking compliance. It did not change the requirement, the score you post, or your liability if that score is wrong.

A Practical Framework: Five CMMC Compliance Moves That Work in Every Scenario

Whether Phase II restarts as written, restarts in a narrower form or is redesigned, these steps pay off.

1. **Find your CUI.** Map where CUI enters, lives and leaves. Most suppliers find it in more places than expected.
2. **Shrink the boundary.** A dedicated CUI enclave can reduce the number of users, devices and systems in scope, and with them the cost to secure and assess.
3. **Make the SPRS score true.** Score again against all 110 Revision 2 requirements using evidence, not memory. Fix or document gaps in a plan of action and milestones.
4. **Keep the paperwork current.** An accurate System Security Plan, incident response plan and evidence binder are what any assessor, prime contractor or investigator will ask for first.
5. **Watch for Revision 3.** The task force recommended finalizing the move to NIST SP 800-171 Revision 3. Design new controls so they can map to it.

The Cost of Doing Nothing

- **Enforcement risk does not pause.** An overstated SPRS score is a representation to the government whether or not a C3PAO ever checks it.
- **Primes are still asking.** Prime contractors carry flow down obligations and may require evidence from suppliers.
- **A compressed restart.** If Phase II resumes for a narrower population, the suppliers in that population may face a short window and competition for assessor time.
- **Rework.** Security spending that is stopped and restarted costs more than a steady plan.

A simple way to frame it for leadership: (value of CUI contracts at risk) multiplied by (likelihood of being unable to show compliance when asked), plus the cost of an emergency remediation project later.

How Norseman Helps

Norseman has delivered for the Department of War, the Intelligence Community and federal civilian agencies since 1992, in environments where the adversary is a nation state. We are ourselves CMMC Level 2 compliant and certified to ISO/IEC 27001, so we work under the same kind of requirements we help clients meet. We bring that rigor to defense suppliers and to commercial manufacturers with defense work.

- **Engage and assess:** We start with your contracts, your people and your data flows, and find where CUI actually lives.
- **Design:** We design the smallest defensible enclave, choosing from more than 300 technology vendors on a vendor neutral basis.
- **Integrate and test:** We validate the build in our Annapolis Junction integration lab before it reaches your users.
- **Support:** We stay with you to keep evidence current, so that your score stays true.

Norseman is not a C3PAO and does not perform certification assessments.

Book a CUI Enclave Scoping Workshop

Know where your CUI lives before anyone asks. In one working session and a written follow up, we will map your CUI, size your smallest defensible boundary and show what it takes to stand behind your SPRS score.

Scope my enclave

This article is general information, not legal advice. Consult counsel about your specific contractual obligations.

Frequently Asked Questions

Is CMMC Phase II cancelled?

No. DoW suspended Phase II on July 13, 2026 and is reviewing the program. As of early November 2026, no restart date had been announced, and a task force option under discussion would restart it for a narrower group of contractors.

Do I still need to post a NIST SP 800-171 score in SPRS?

Yes, where your contract includes DFARS 252.204-7019 or 7020. Phase I self assessment requirements also remain in place. Confirm your obligations with your contracting officer or counsel.

Can a CUI enclave reduce compliance cost?

Often yes. Placing CUI and the people who use it in a smaller environment reduces the number of systems to secure and assess. Whether it is cheaper depends on how widely CUI is used across your business.

Related

- **CUI Enclave for Defense Suppliers While CMMC Rules Settle**
- **Cyber Resilience and Zero Trust**
- **How we work**
- **Executive Briefing Center and integration lab**
- **Support**

Sources

- **Department of War release, "Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements," July 13, 2026**
- **Jenner and Block, "Department of War Suspends CMMC Phase II, But Compliance Obligations Remain," July 14, 2026**
- **Morgan Lewis, "Department of War Suspends CMMC Phase II Requirements, but Cybersecurity Obligations Remain," July 16, 2026**
- **Latham and Watkins, "What Defense Contractors Should Know About DOD's Suspension of CMMC Phase 2," July 30, 2026**
- **SBA Office of Advocacy, "DoW Requests Information for CMMC Reform Task Force," July 20, 2026**
- **Washington Technology, "CMMC's Phase 2 suspension locked in with binding regulation," September 2026**
- **Federal News Network, "DoD's reasons for CMMC pause falling apart in face of RFI responses," October 26, 2026**
- **Federal News Network, "RFI offers path forward for DoD with CMMC," October 27, 2026**

Published at norseman.com/insights/cmmc-phase-2-suspended-nist-800-171. To talk with Norseman Defense Technologies, call 410.579.8600 or email sales@norseman.com.