

Self-Assessment Is Now Written into the Contract. Your Risk Isn't.

Why DARS Class Deviation 2026-00025, Revision 3 Locks in the CMMC Pause Without Removing the Underlying Obligation to Protect CUI

CMMC 2.0

DFARS 7012

NIST SP 800-171

False Claims Act

The Challenge

DARS Class Deviation 2026-00025, Revision 3 formally writes the July 13, 2026 CMMC Phase 2 suspension into the DFARS Part 240 text itself. Contracting officers must now strip or revise CMMC requirements in new and existing solicitations, and CMMC Level 1 and Level 2 can be satisfied as Self assessments in procurement documents. In the market, that reads as pressure off. Read closely, the memo says nothing of the kind: baseline compliance still runs through NIST SP 800-171 Rev 2 under DFARS 252.204-7012, and Revision 3 explicitly frames the change as tied to a pending CIO memo and active litigation, not a rule change to the underlying data protection requirement.

The Solution

Kiteworks helps Defense Industrial Base contractors close the gap between a codified self-assessment posture and the security substance a returning CMMC Phase 2 will demand. The platform is FedRAMP High In Process, FedRAMP Moderate Authorized since 2017, supports 90% of CMMC 2.0 Level 2 requirements out of the box, and is FIPS 140-3 validated, giving contractors verifiable evidence behind every self-attested SPRS score rather than a paper claim alone.

What Revision 3 Actually Locks In

180 Days

Max Validity For A Conditional CMMC
Level 2 Or 3 Status

3 Years

Max Validity For A Final CMMC Level 2 Or
3 Status

14 Days

Business Days To Rebut A Government
Assessment Finding

Why Self-Assessment Alone Isn't Enough



No Third-Party Check on Your Own Claims

Revision 3 permits CMMC Level 1 and Level 2 as Self assessments, which removes independent verification. Contractors carry the full weight of their own SPRS score's accuracy.



DFARS 252.204-7012 Never Paused

The memo's own text keeps the obligation to safeguard covered defense information under NIST SP 800-171 Rev 2 fully in force, regardless of the CMMC phase-in timeline.



The Suspension Is Explicitly Temporary

Revision 3 ties the CMMC change to a CIO memo and an active federal court order, not a permanent rule. Contracting officers must still amend active solicitations and modify existing contracts as the underlying posture evolves.

What Self-Attestation Doesn't Protect You From

Self-assessment lowers the bar for entry, not the bar for exposure. Revision 3 preserves every one of the following government levers alongside the Self option.



False Claims Act Exposure

A self-attested CMMC status posted to SPRS is a representation the government relies on for award, option, and renewal decisions. With no independent check before that score is used, the accuracy risk sits entirely with the contractor who made the claim.



Government Assessment Authority Stays Fully Active

Revision 3 preserves DoW's authority to conduct Medium and High NIST SP 800-171 DoW Assessments on any covered contractor information system, self-assessed or not. When DCMA conducts one, its results take precedence over any other assessment on record, including a contractor's own Self status.



Only 14 Business Days to Rebut an Adverse Finding

Once a Medium or High assessment concludes, DoW posts a summary score to SPRS visible to DoW Components. The contractor gets 14 business days to submit missing evidence or rebut the findings before that score stands as the record.



Award and Option Exercise Both Hinge on a Current Status

Contracting officers must check SPRS before award, before exercising an option, and before extending a period of performance, and must withhold all three if the CMMC status has lapsed. A status that goes stale mid-contract can stall a renewal just as easily as it can block new business.



Existing CMMC Contract Language Doesn't Vanish on Its Own

Revision 3 directs contracting officers to strip Phase 2 requirements from active contracts, but only prior to the next option exercise or the next scheduled administrative modification. Until that modification happens, the original contract language, and the underlying data-protection clause, stays in force.

Ready to Back Your Self-Attestation With Real Evidence?

www.kiteworks.com

Kiteworks



Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.