The Department of War Just Gave Defense Contractors a CMMC Snow Day

The suspension reached Phase II rather than the obligation to protect CUI and defend the next affirmation.

David W. Koran

CyberAB Registered Practitioner Advanced

July 15, 2026

On July 13, 2026, the Department of War suspended the transition to Phase II of the Cybersecurity Maturity Model Certification program. Phase II had been scheduled to begin on November 10, 2026, and would have expanded the use of CMMC Level 2 third-party assessments and Level 3 government assessments across the Defense Industrial Base [1]. The suspension functions as a snow day: the examination has been postponed, and the material it examines has not changed.

The suspension is a beneficial outcome for contractors facing a third-party assessment on a fixed date, particularly small manufacturers being pushed toward rushed enclave purchases or long-term service agreements they could not justify. It does not alter any underlying obligation. The requirements of NIST SP 800-171, the safeguarding obligations of DFARS 252.204-7012, the self-assessment and affirmation requirements, and False Claims Act exposure all remain in force. This paper describes what was suspended, what remains, what the enforcement record shows, and how contractors should use the interim period.

What the Suspension Removed

The November 10 date was never a universal certification deadline. It marked the beginning of the next acquisition phase, during which additional solicitations and contracts may require a Level 2 C3PAO or Level 3 DIBCAC assessment.

The operative instructions are in the memorandum implementing the suspension, signed by Kirsten A. Davies, the Department of War Chief Information Officer. Program Managers and requiring activities may designate only CMMC Level 1 (Self) or Level 2 (Self), and may not designate Level 2 (C3PAO) or Level 3 (DIBCAC). Active solicitations carrying those requirements are to be amended, and contracting officers are directed to remove them from existing contracts by modification prior to the exercise of the next option period or during the next scheduled administrative modification. No waivers will be granted during the review, and further guidance is to be issued at the conclusion of the 60-day review [2].

What Remains in Force

Contractors hold one of two kinds of SPRS records, and sometimes both. The older record is the Basic NIST SP 800-171 DoD Assessment score, submitted under DFARS 252.204-7019 [5] and DFARS 252.204-7020 [6]. Most contractors have this one, and the score must be current, meaning no more than three years old, before a contracting officer can consider the company for award. The newer record is CMMC Level 2 (Self), which applies when a contract requires that status. It carries its own CMMC scoping

rules, a self-assessment every three years, an annual affirmation by a senior official, and six-year retention of the supporting evidence [3]. The two records measure related requirements, and neither substitutes for the other.

The suspension revised neither record. An inaccurate Basic Assessment score remains inaccurate. An unsupported Level 2 self-assessment and affirmation remain unsupported. The first task for any contractor is to establish which representations it has made, what evidence supports them, and when they come up for renewal.

The Department has stated that Phase I self-assessment requirements remain in place, that it will enforce NIST SP 800-171 Revision 2 through self-assessments and selected government-led assessments during the review period, and that contractors and subcontractors remain responsible for safeguarding covered defense information under DFARS 252.204-7012 [1][4]. Chief Information Officer Davies made the same point at the Pentagon media roundtable announcing the suspension, telling reporters that the action "does not eliminate the legal requirement" for industry partners to protect federal data [13]. DFARS 252.204-7020 continues to require applicable subcontractors to maintain at least a current Basic Assessment before subcontract award and preserves the Government's authority to conduct Medium and High assessments [6].

What the Enforcement Record Shows

Unverified self-reported scores have a documented reliability problem. The two matters below were resolved by settlement. The claims resolved are allegations, and the settlements are not determinations of liability [10].

Contractor	Score submitted	Score determined by outside review	How the difference surfaced
MORSECORP Inc.	104, January 2021	Negative 142, July 2022	Gap analysis performed by a third-party cybersecurity consultant the company engaged
LOGZONE Inc.	110, October 2021	Negative 170, 2024	Assessment conducted by the Defense Contract Management Agency

Self-reported SPRS scores compared with scores determined by outside review, as alleged in the resolved matters [7][8][11].

The Government alleged that MORSECORP Inc. submitted a score of 104 in January 2021, that a third-party cybersecurity consultant notified the company in July 2022 that its actual score was -142, and that the reported score remained unchanged until June 2023. The company paid $4.6 million [7]. LOGZONE Inc. is alleged to have reported a

perfect 110 in October 2021, in contrast to a Defense Contract Management Agency assessment result of -170. The company paid $507,144 in June 2026 [8][11]. The gaps were 246 and 280 points, and in neither case did the company identify its own. A consultant identified one, and the Government identified the other.

The cause of an inaccurate score is usually ordinary rather than dishonest. Scoring under the DoD Assessment Methodology is binary. Multifactor authentication deployed for administrators but not for every user who touches CUI is not implemented. Encryption applied to some file shares and not others is not implemented. A policy that does not describe what the organization actually does is not implemented. A requirement can appear substantially complete from inside the company and still fail an assessment objective.

Enforcement did not pause with the program. False Claims Act settlements and judgments reached $6.8 billion in the fiscal year ending September 30, 2025, including over $52 million across nine cybersecurity fraud settlements, a category the Department of Justice reports has more than tripled in each of the past two years [10][15]. The exposure in these matters arises from billing the Government against requirements the company had not met; the reported score is evidence of what the company knew when it billed. A truthful low score does not cure the underlying noncompliance, and declining to examine the score offers no protection, because the statute reaches deliberate ignorance and reckless disregard and requires no proof of specific intent to defraud [12]. Company size is not a mitigating factor: in December 2025, an Illinois precision machining company paid $421,234 to resolve allegations that it failed to provide adequate cybersecurity, as required by DFARS 252.204-7012 [4], for technical drawings supplied to defense prime contractors, in a case brought by a former quality control manager [9].

The Suspension Removed the Verification Mechanism

The C3PAO assessment was the independent verification gate at the end of the compliance process. The approaching gate prompted corrective action: contractors engaged outside professionals, corrected the scope, reviewed System Security Plans, remediated deficient controls, and assembled evidence because an independent party would eventually test the result. The score was typically fixed before it was tested.

Without a scheduled examination, that correction does not occur on its own. In most small and mid-sized contractors, the same people who built and administer the environment also write the documentation and score the self-assessment, and a senior

official affirms the result relying on both. The arrangement is often the only one available, and it makes the team's own assumptions difficult to identify from inside. The suspension therefore does not reduce attestation risk. It removes the process that was reducing it, and it leaves the affirmation in place.

In my article in the July 2026 issue of National Defense, I compared the CMMC assessment capacity problem to the Y2K remediation effort in financial services [16]. That industry met its deadline through coordinated action, regulatory flexibility, and clear communication about the required result, and it mobilized because midnight could not be moved. The Department of War just moved midnight. That relieves the capacity problem the article described, but it also removes the one thing that made the Y2K mobilization happen. Contractors now face the same underlying work without a date forcing it.

The Next Affirmation Is the Decision Point

Every contractor with a Level 2 self-assessment obligation will submit an affirmation again. The affirming official is a senior company representative. The affirmation states that the security requirements are implemented and will continue to be implemented, is entered into SPRS where the Department verifies it for solicitation and contract eligibility, and must be supported by evidence retained for six years. A subsequent government assessment can replace the self-reported result [3].

The question before the next affirmation is whether the number in SPRS reflects the existing environment and whether the company can provide evidence to support it. If the answer is yes, the affirmation is routine. If the answer is no or unknown, the affirmation renews an inaccurate representation with a current date. The suspension is the interval in which that question can be answered before the signature rather than after.

Use of the Interim Period

The sequence is straightforward. Confirm which contracts and systems involve CUI. Correct the CMMC scope to match that answer. Perform the Level 2 self-assessment against NIST SP 800-171A rather than against the requirements' summary language. Remediate the material deficiencies the assessment exposes. Retain objective evidence that the requirements operate in practice. Obtain an independent review that challenges it all. Submit the score and the management affirmation when both can be defended. The suspension provides enough time to complete this in the correct order.

An independent consultant can challenge the scope, test the self-assessment results against NIST SP 800-171A, examine the evidence, and compare the documented posture to the operating environment. A consultant cannot issue a CMMC status or make the company's affirmation. The company corrects what the challenge exposes, and the authorized official submits the affirmation and remains responsible for it. The review compares the System Security Plan with the configuration and identifies the evidence that would need to be produced if a DIBCAC team or a prime contractor requested it. The value of this work does not depend on the Reform Task Force's recommendations, because every model under discussion measures the contractor's actual environment against NIST SP 800-171.

Market conditions favor doing this work now. During the run-up to Phase II, readiness work was performed under deadline pressure and priced accordingly. Contractors now have room to evaluate providers, properly scope the work, and sequence remediation against operating and budget constraints, rather than against a reserved assessment date.

Two cautions apply. Contractors should avoid making large commitments based on assumptions about the revised program; a platform purchase, an outsourced enclave, or a multi-year service agreement should solve an identified problem in a known environment. And nothing already built should be removed. Multifactor authentication, segmented networks, controlled administrative privileges, accurate scoping, a defensible System Security Plan, and retained evidence remain relevant under self-assessment, government-led assessment, prime contractor review, or any likely replacement program. Dismantling working controls would lower the real score while the affirmation continues to represent otherwise.

Prime Contractor Requirements Are a Separate Obligation

The suspension does not automatically cancel CMMC requirements issued by prime contractors. Where a prime required Level 2 C3PAO certification solely because the government contract contained that requirement, removal of the upstream requirement should cause the prime to reconsider the subcontract requirement, and the subcontractor should obtain that change in writing. A department-wide memorandum does not amend an executed purchase order. Where the prime has established certification as an internal supplier qualification requirement, it may continue to require additional evidence before releasing CUI.

The prime's position is constrained. A prime is responsible for ensuring that applicable subcontractors hold the CMMC status appropriate to the information they will receive, and prime contractors do not have access to subcontractor information in SPRS [14]. During the suspension, the prime makes that determination without the certification gate that would have answered it. Some primes will respond by expanding their oversight through questionnaires, SSP reviews, evidence requests, and audit rights, resulting in several distinct supplier-assurance processes rather than a single standardized assessment. A supplier whose environment has already been reviewed against the assessment objectives can answer those requests from a single position; a supplier that has not done the work will answer each prime differently.

The 60-Day Review

The CMMC Reform Task Force is collecting industry feedback through a public Request for Information issued alongside the suspension, with responses due by 12 PM Eastern on August 14, 2026, and will deliver recommendations to the CIO within 60 days [1][17]. The RFI asks contractors to identify their most prohibitive cost drivers; the controls that deliver the most actual risk reduction and the least; how the Department might recognize existing commercial cybersecurity capabilities within a compliance framework; and how self-assessment could be streamlined. The task force recommendations may require new guidance, contract changes, or formal rulemaking before implementation. Phase II does not automatically return on the sixty-first day, and no rescheduled date has been published.

The Department could restore third-party assessments with limited changes, narrow the population of contracts requiring certification, base verification on CUI sensitivity, increase government-led sampling, or shift more supplier oversight toward prime contractors. Greater reliance on government-led assessment warrants attention, as it is the mechanism that produced the LOGZONE result. If the replacement model directs assessment resources toward high-risk programs, poor scores, or questionable representations, the population most exposed under the new model is the population least prepared under the old one.

Conclusion

The suspension of CMMC Phase II removed a scheduled third-party examination. It did not revise any SPRS record, relieve any safeguarding obligation under DFARS 252.204-7012, or affect False Claims Act exposure, which arises from billing the Government against requirements a company has not met. None of the enforcement

outcomes described in this paper involved a breach; each involved a representation the environment did not support and claims submitted while it stood.

Contractors that use the interim period to confirm their scope, complete implementation, assemble evidence, obtain an independent challenge of the results, and affirm a number management can defend will be prepared for whatever verification model follows the review. Contractors that suspend their own compliance work, along with the program, will return to the same requirements with the same deficiencies and less time.

About the Author

David W. Koran holds the CyberAB Registered Practitioner Advanced credential and is the founder of a consulting practice serving Defense Industrial Base contractors and the legal counsel who represent them. The practice focuses on CMMC readiness, enablement, and implementation, including System Security Plan development and assisting companies in accurately reporting their SPRS scores. He is an Associate Member of the American Bar Association Section of Public Contract Law and the author of The CMMC Decision.

He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

[1] U.S. Department of War, *Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements*, July 13, 2026. war.gov/News/Releases/Release/Article/4542329

[2] U.S. Department of War, Office of the Chief Information Officer, *Implementing Suspension of CMMC Phase II*, memorandum 26-P-1023, Attachment 1, signed July 10, 2026 and released July 13, 2026. dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf

[3] 32 CFR 170.16, *CMMC Level 2 self-assessment and affirmation requirements*. ecfr.gov/current/title-32/part-170/section-170.16

[4] DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*. acquisition.gov/dfars/252.204-7012

[5] DFARS 252.204-7019, *Notice of NIST SP 800-171 DoD Assessment Requirements*. acquisition.gov/dfars/252.204-7019

[6] DFARS 252.204-7020, *NIST SP 800-171 DoD Assessment Requirements*. acquisition.gov/dfars/252.204-7020

[7] U.S. Department of Justice, *Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations*, March 26, 2025. justice.gov/opa/pr/defense-contractor-morsecorp-inc-agrees-pay-46-million-settle-cybersecurity-fraud

[8] U.S. Department of Justice, *Alabama Defense Contractor Agrees to Pay $507,144 to Resolve False Claims Act Liability Relating to Cybersecurity Violations*, June 18, 2026. justice.gov/opa/pr/alabama-defense-contractor-agrees-pay-507144-resolve-false-claims-act-liability-relating

[9] U.S. Department of Justice, *Illinois Precision Machining Company Agrees to Pay $421,234 to Resolve Alleged False Claims Act Violations*, December 2025. justice.gov/opa/pr/illinois-precision-machining-company-agrees-pay-421234-resolve-alleged-false-claims-act

[10] U.S. Department of Justice, *False Claims Act Settlements and Judgments Exceed $6.8B in Fiscal Year 2025*, January 16, 2026. justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-68b-fiscal-year-2025

[11] Crowell & Moring LLP, *LOGZONE's $507K FCA Settlement: How DIBCAC Scores Are Now Driving DOJ Enforcement*, July 2026. crowell.com/en/insights/client-alerts/logged-out-how-logzones-dibcac-challenges-put-it-squarely-in-dojs-crosshairs

[12] 31 U.S.C. 3729, *False claims*, subsection (b)(1). govinfo.gov/link/uscode/31/3729

[13] Breaking Defense, *Pentagon announces 'immediate suspension' of CMMC Phase II mandates*, July 13, 2026, reporting remarks by the Department of War Chief Information Officer at a Pentagon media roundtable. breakingdefense.com/2026/07/pentagon-announces-immediate-suspension-of-cmmc-mandates

[14] Wiley Rein LLP, *DOD Issues Final DFARS Rule for Cybersecurity Maturity Model Certification Program*, September 2025, reporting the Department's confirmation that prime contractors will not have access to subcontractor information in SPRS.

wiley.law/alert-DOD-Issues-Final-DFARS-Rule-for-Cybersecurity-Maturity-Model-Certification-Program

[15] U.S. Department of Justice, *Fact Sheet: False Claims Act Settlements and Judgments, Fiscal Year 2025*, January 16, 2026, accompanying the recovery announcement at reference 10. justice.gov/opa/media/1424126/dl

[16] David W. Koran, *Viewpoint: Industry Should Apply Y2K Lessons Learned to CMMC Crunch*, National Defense, July 2026. nationaldefensemagazine.org/articles/2026/7/2/industry-should-apply-y2k-lessons-learned-to-cmmc-crunch

[17] U.S. Department of War, *Request for Information: Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base*, approved for distribution July 13, 2026. Responses due August 14, 2026. davidkoran.com/dow-cio-dod-information/dow-cmmc-suspend-questionnaire.pdf