PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

The Certificate Requirement Is Paused. The Liability Is Not.

What the CMMC Phase 2 pause changes—and what it doesn't

By Nick DeLena, Partner

The Department of War announced, on July 13, 2026, the immediate suspension of CMMC Phase 2. That requirement, scheduled to take effect November 10, 2026, would have made third-party certification a condition of award for contracts involving Controlled Unclassified Information. Pending and future implementation milestones are suspended as well; contracting officers have been directed to amend active solicitations to remove Level 2 (C3PAO) and Level 3 (DIBCAC) requirements; and a new CMMC Reform Task Force will deliver recommendations on the program's future within 60 days.

If you are a decision maker at a company that holds defense contracts, your inbox is already full of alerts summarizing the announcement. Most of them bury the point that matters. So let me say it plainly, as someone who leads a C3PAO practice and conducted numerous CMMC Level 2 assessments: **Nothing about your obligation to protect federal data changed on July 13. What changed is who is accountable when you fall short. The answer is now, more than ever: you.**

What Was Actually Suspended

CMMC was never the security requirement. The requirement has been in your contracts since 2017 through DFARS 252.204-7012, which obligates every contractor and subcontractor handling covered defense information to implement the 110 controls of NIST SP 800-171, report cyber incidents within 72 hours, and use FedRAMP Moderate (or equivalent) cloud services for systems touching CUI. CMMC was the verification layer: the mechanism the Department of War established to verify contractor compliance.

That verification layer is what's paused. The underlying rules, 32 CFR Part 170 and the DFARS acquisition rule, remain on the books, and removing them would require formal rulemaking measured in months, not weeks. Phase 1 remains fully in force: if your contracts require a Level 1 or Level 2 self-assessment, you must still perform it, post your score to SPRS, and, critically, have a senior official affirm continuing compliance.

During the review period, the Department has said it will enforce NIST SP 800-171 Rev 2 through self-assessments and select government-led assessments. Read that second clause twice. DIBCAC did not close. The government reserved the right to show up and check.

Why CMMC Exists in the First Place

The government's own assessment data reinforced the survey findings. In a study presented by DCMA's Defense Industrial Base Cybersecurity Assessment Center in March 2023, DIBCAC compared contractors' self-reported SPRS scores against the results of its own Medium assessments, which consist of a documentation review rather than on-site verification. Across the study population, the average self-reported score was 56; the average score after DIBCAC's review was negative 58, a swing of more than 110 points on a 313-point scale. One contractor's score moved from a self-reported 110, the maximum possible, to 7. Another fell from negative 23 to negative 203, the lowest score the methodology allows.

The same presentation contained a telling behavioral detail. After DIBCAC publicly announced the Medium assessment study, it compared SPRS data from March 2022 against data from July 2022 and identified 156 entries whose scores had declined by at least 100 points, including one contractor that revised its own score from 110 to negative 203. In other words, a meaningful number of contractors corrected their attestations only once they believed the government might verify them. DIBCAC's assessments of the most commonly failed requirements, drawn from 117.

High assessments conducted between 2019 and 2022, found foundational controls at the top of the list: FIPS-validated cryptography, multifactor authentication, and flaw remediation. These are not exotic requirements. They are the basics, and the gap between attestation and implementation is precisely the problem any successor framework must solve.

Data Cited by the SBA Is Inaccurate

Any review is only as sound as the data beneath it, and the numbers circulating in support of this suspension deserve a closer look. The SBA's statement commending the decision cites compliance costs approaching $593,800 for firms requiring third-party assessment and $388,600 for those eligible for self-assessment. The Department's own regulatory analysis for the CMMC final rule tells a different story: approximately $104,670 for a small entity's certification over a full three-year cycle, and roughly $37,000 for a self-assessment. The gap exists because the Department deliberately excluded implementation costs, which have been contractual obligations since the FAR safeguarding clause in 2016 and the DFARS requirement to implement NIST SP 800-171 by the end of 2017.

The larger figures can only be reached by attributing to CMMC the cost of protecting federal data itself, an obligation the suspension does not touch and no contractor should treat as relieved. The capacity argument has similar difficulties: the claim that more than 120,000 small businesses would be forced through a system of roughly 100 assessors confuses the numbers. There are approximately 110 C3PAO organizations, who employ approximately 1,500 CMMC certified assessors. Assessor capacity is not currently a constraint on the ecosystem – OSC readiness is.

The Risk Didn't Shrink − It Moved

Under the Phase 2 model, a contractor's compliance story would have rested on a certificate issued by an independent assessor after a rigorous, evidence-based examination, in addition to self-attested scores. Imperfect and expensive, yes. But it put a qualified third party in the mix between your executives and the government's enforcement apparatus.

That buffer is gone. In a self-attestation regime, the compliance story rests entirely on a score your organization calculated and an affirmation your executive signed. The Department of Justice's Civil Cyber-Fraud Initiative has spent four years using the False Claims Act against contractors whose cybersecurity representations didn't survive scrutiny, and there is no reason to expect it will treat SPRS affirmations differently. If anything, the suspension raises the stakes: with third-party certification potentially off the table, a self-assessed score is the representation that the government and qui tam relators will test.

Ask yourself one question: if a DIBCAC assessor or a DOJ investigator examined your environment tomorrow, would the evidence support the score in SPRS today? If you hesitated, the suspension did not make your life easier. It shifted even more responsibility to your affirming official.

Your Readiness Investment Was Not Wasted

Contractors that spent the last two years preparing for certification are understandably frustrated. Department leadership addressed this directly, with the CIO telling reporters that forward-leaning companies contributed to national security and that the money was not spent in vain. Set the reassurance aside and look at the economics: everything you built (the enclave, the SSP, the evidence discipline, the POA&M hygiene) is exactly what defends a self-assessment under government or DOJ scrutiny, and exactly what will satisfy whatever verification model replaces Phase 2. The deadline moved. The asset didn't depreciate.

There's a competitive angle, too. Primes carry their own 7012 flowdown obligations and did not stop caring about subcontractor security on July 13. Expect sophisticated primes to fill the verification vacuum contractually, and expect demonstrable, independently validated compliance to become a discriminator precisely because the government temporarily stopped requiring it.

What to Do in the Next 60 Days

First, do not stand down your compliance program. Every plausible outcome of the review, whether restored deadlines, narrowed certification thresholds, government-led verification, or a restructured program, keeps NIST SP 800-171 as the substantive standard. Build to the standard; stay flexible on the mechanism.
Second, treat your next SPRS submission like it will be audited, because it may be. Validate the score independently before an executive affirms it. A mock assessment conducted to C3PAO standards is now less about certification prep and more about attestation defense.

Third, be heard. The Department has issued a Request for Information seeking industry input on cost drivers, administrative burden, and which controls deliver genuine risk reduction. Responses are due August 14. The Reform Task Force will synthesize that feedback into its recommendations. If the current model burdened you, or if third-party assurance protected you, this is the moment the record gets written. Companies that stay silent will live under a framework designed around other people's comments.

Fourth, watch mid-September. The task force report lands roughly 60 days from the announcement, and it, not the July 13 memo, will tell you what the next decade of defense cybersecurity compliance looks like.

The Longer View

This is the second time in five years the Department has paused CMMC to rethink it; the 2021 review produced a streamlined CMMC 2.0 rather than a repeal. Whether history repeats is genuinely uncertain, and officials have pointedly declined to rule out any outcome. But across every administration, every leadership change, and now two program-wide reviews, two things have never wavered: the contractual obligation to safeguard federal data, and the government's willingness to pursue those who claim compliance they don't have.

The certificate requirement is temporarily suspended. The underlying standard, the DFARS 252.204-7012 contract clause, and the consequences are not. Govern yourselves accordingly.

Although Phase 2 certification is temporarily suspended as a contract requirement, C3PAOs continue to perform voluntary CMMC assessments for organizations seeking independent validation of their cybersecurity programs. Our team includes certified **CMMC** assessors and advisors who have guided defense contractors through every phase of the program's evolution from its origins in 2015. If you're reassessing your compliance posture in light of the suspension, we should talk.

Contact Us

If you have any questions, please contact your client service team or:

Nick DeLena, CISSP, CISA, CRISC, CDPSE, CMMC Lead Assessor
Partner
ndelena@pkfod.com

This article was originally published on July 20, 2026.