Articles + Publications | July 16, 2026

Years in the Making, Suspended in a Day: DoD/W Halts CMMC Phase II but Keeps Baseline Cybersecurity Obligations

WRITTEN BY

Michael E. Barnicle | Hilary S. Cairnie | Peter E. Jeydel | Lu Reyes | Bryan R. Williamson | Bonnie Gill | Anthony Pappas | Trey Smith

KEY POINTS

- DoD suspended CMMC Phase II on July 13, 2026, halting the November 10, 2026, deadline and all related implementation milestones pending a comprehensive reform review by a newly established CMMC Reform Task Force.
- CMMC Level 2 (C3PAO) and Level 3 (DIBCAC) third-party assessment requirements are suspended, and active solicitations and contracts must be amended to remove those designations during the suspension period.
- Core cybersecurity obligations remain enforceable: DFARS 252.204-7012, NIST SP 800-171 Rev. 2 compliance, cloud security requirements, and cyber incident reporting duties are all still in effect.
- The SBA estimates CMMC third-party certification costs can reach approximately $593,800 per small firm, a burden cited as a key driver of the suspension and of small contractor attrition from the defense industrial base.
- Defense contractors have until August 14, 2026, to submit RFI responses and directly influence the design of the reformed CMMC program.

On July 13, 2026, the U.S. Department of Defense/War (DoD/W) announced the immediate suspension of Cybersecurity Maturity Model Certification (CMMC) Phase II requirements — scheduled to take effect on November 10, 2026 — pending a top-to-bottom review by a newly established CMMC Reform Task Force. The announcement, formally titled “Removing Barriers to Defense Industrial Base Expansion: Immediate Suspension and Strategic Review of Cybersecurity Maturity Model Certification Requirements,” came as a surprise reversal after years of rulemaking activity stretching back to 2019. In addition to the announcement, DoD/W published an implementation memo outlining the procedural rollout of the CMMC suspension. For defense contractors and their compliance teams, the suspension raises immediate practical questions about what changes, what remains, and what comes next.

1. KEY TAKEAWAYS FOR DEFENSE CONTRACTORS

- **Phase II is suspended immediately.** The November 2026 deadline for CMMC Phase II transition is suspended, and all pending and future CMMC implementation milestones across DoD/W solicitations and contracts are held in abeyance until further notice.
- **Phase I and II self-assessment requirements remain in effect.** CMMC Level 1 (Self) and Level 2 (Self) assessments are still required. Program managers and requiring activities may only designate these two assessment types in solicitations and contracts going forward.

- **Third-party certification requirements are off the table for now.** CMMC Level 2 (C3PAO) and Level 3 (DIBCAC) assessments may not be designated during the suspension period. Active solicitations and contracts containing these requirements must be amended or modified to remove them.
- **Core DFARS cybersecurity obligations remain.** The suspension does not affect contractors' foundational cybersecurity obligations. DoD/W will continue enforcing baseline compliance with NIST SP 800-171 Rev. 2. Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is still in effect, as are NIST SP 800-171 Rev. 2 compliance requirements, cloud security obligations, and cyber incident reporting duties.
- **Industry has a 60-day window to shape the future program.** DoD/W has issued a request for information (RFI) seeking industry feedback on reforming CMMC by utilizing existing commercial cybersecurity capabilities, optimizing self-attestation capabilities, and streamlining cybersecurity compliance requirements. Responses are due August 14, 2026.

2. WHY DOD/W ACTED

The suspension reflects mounting pressure from small business stakeholders, the Small Business Administration (SBA), and the Defense Industrial Base (DIB) at large. DoD/W's announcement cited "prohibitive compliance costs, severe shortages in third-party assessment capacity, and complex regulatory timelines" as structural incompatibilities with its goal to rapidly expand the defense industrial base. The SBA, which issued its own commendation of the suspension, estimates that CMMC compliance costs can reach approximately $593,800 per certification for small firms requiring third-party assessment, and approximately $388,600 for firms eligible for self-assessment — burdens the SBA states have caused many small contractors to exit or consider exiting defense work entirely.

3. THE CMMC REFORM TASK FORCE AND WHAT COMES NEXT

DoD/W's chief information officer is immediately establishing a CMMC Reform Task Force charged with conducting a 60-day comprehensive review of the certification program. Its mandate: recommend a reformed cybersecurity framework that accelerates capability, reduces barriers for small and nontraditional businesses, and replaces costly third-party compliance models with scalable security measures.

4. PRACTICAL GUIDANCE AND RECOMMENDATIONS

- **Do not stand down on cybersecurity compliance.** DFARS 252.204-7012 obligations, NIST SP 800-171 Rev. 2 requirements, and Level 1 and 2 self-assessment requirements remain intact and enforceable.
- **Review active solicitations and contracts.** If your solicitation or contract currently requires CMMC Level 2 (C3PAO) or Level 3 (DIBCAC) certification, expect — and monitor for — amendments and modifications from the contracting activity removing those requirements.
- **Consider participating in the RFI.** The DoD/W RFI (Notice ID: DoDCIOReformingCMMCforDIB001, due August 14, 2026) presents a direct opportunity for contractors to influence how the reformed CMMC program is designed.
- **Stay alert to Task Force recommendations.** The Task Force's 60-day review will conclude with reform recommendations that could significantly reshape CMMC requirements. Contractors should monitor announcements closely and be prepared to adapt compliance strategies accordingly.

RELATED INDUSTRIES + PRACTICES

- Corporate
- Government Contracts
- Privacy + Cyber