JENNER & BLOCK

Department of War Suspends CMMC Phase II—But Compliance Obligations Remain, As Does Enforcement Risk

Client Alerts

July 14, 2026
By: David Robbins, Moshe B. Broder, Matthew L. Haws

On July 13, 2026, the Department of War (DoW) announced the immediate suspension of the Phase II requirements of the Cybersecurity Maturity Model Certification (CMMC) program, which had been scheduled to take effect on November 10, 2026. The suspension, memorialized in a memorandum dated July 10, 2026, and signed by DoW Chief Information Officer Kirsten Davies, also halts the pending Phase III and Phase IV implementation milestones and directs a comprehensive, 60-day review of the program.

For contractors that have spent the past several years—and considerable resources—preparing for third-party certification, the announcement is significant. But it should not be mistaken for a reprieve. The obligation to protect covered defense information has not been suspended, only one specific mechanism for verifying it. As we noted in our last CMMC alert in 2024, contractors are still obligated to comply with the underlying cybersecurity requirements, and enforcement of non-compliance under existing contractual obligations continues to increase.

As background, and to recap our prior updates on this subject, DoD's August 15, 2024 proposed rule signaled that CMMC was moving from aspiration to contractual obligation, and the acquisition rule was subsequently finalized and took effect in November 2025 under a phased, three-year rollout. Phase I—which commenced on November 10, 2025—required offerors on applicable solicitations to complete and post CMMC Level 1 or Level 2 self-assessments in the Supplier Performance Risk System (SPRS). Phase II, the milestone now suspended, would have introduced the requirement that contractors handling controlled unclassified information (CUI) achieve CMMC Level 2 certification through an assessment by an accredited Certified Third-Party Assessment Organization (C3PAO) as a condition of award. Phase III, slated for November 2027, would have layered in Level 3 assessments conducted by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC); it, too, is suspended, as is full implementation under Phase IV.

The stated rationale is cost and industrial-base attrition. The Davies memorandum reasons that the current program, while intended to enhance security, imposes significant and often prohibitive burdens on the Defense Industrial Base (DIB)—particularly the small and non-traditional businesses

that the Department views as critical to innovation and production goals—and that the current implementation model is structurally incompatible with the Department's objective of rapidly expanding the DIB. In announcing the decision, Under Secretary of War for Acquisition and Sustainment Michael Duffey and CIO Davies emphasized the mismatch between the roughly 100,000-plus contractors that would ultimately require assessment and the comparatively limited C3PAO assessment capacity that exists today—a structural compatibility concern that has long loomed over the piecemeal rollout of the CMMC program. The suspension is framed as an implementation of the Secretary of War's directive to cut bureaucratic red tape, reduce acquisition barriers, and accelerate delivery of capability to the warfighter.

Critically for contractors, the suspension does not disturb the baseline. DoW has confirmed that Phase I self-assessment obligations remain in force, as do the existing requirements of DFARS 252.204-7012, which continues to require implementation of the 110 security controls in NIST SP 800-171 Rev. 2 and reporting of cyber incidents. During the review period, DoW will continue to enforce cybersecurity compliance against the NIST SP 800-171 Rev. 2 standard through self-assessments and select government-led assessments, which the Department characterizes as a shift toward tangible cyber hygiene and away from administrative overhead. In short, the third-party certification gate has been lifted; the substantive security requirements behind it have not.

The implementing guidance issued alongside the announcement translates the policy into contractual mechanics. During the suspension, program managers and requiring activities may include only CMMC Level 1 (Self) or Level 2 (Self) assessment requirements in solicitations, and may not include Level 2 (C3PAO) or Level 3 (DIBCAC) requirements. Where a requirements package already contains a C3PAO or DIBCAC requirement, program offices are directed to amend active solicitations to remove it, and contracting officers are instructed to strike such requirements from existing contracts by modification prior to the exercise of the next option period or at the next modification. Contractors with pending bids or in-performance contracts should therefore anticipate solicitation amendments and contract modifications in the near term, and should track those changes carefully against their own compliance postures.

The path forward is a 60-day, top-to-bottom review conducted by a newly established CMMC Reform Task Force, which will synthesize industry feedback and deliver a final report with recommendations within that window. To inform the review, DoW has issued a public Request for Information (RFI) seeking input on cost drivers, the administrative burdens associated with CMMC compliance, which NIST SP 800-171 controls deliver meaningful risk reduction,[1] and how the Department might recognize commercial cybersecurity tools and managed services in lieu of separate assessments. Responses to the RFI are due August 14, 2026. Contractors with a stake in the program's ultimate design—including those that have already invested in readiness—should give serious consideration to submitting comments. In so doing, contractors should refer to the many thoughtful comments submitted by contractors in response to earlier iterations of the CMMC rulemaking.

The suspension also introduces new ambiguities likely to weigh on contractor decision-making. Foremost among them is the durability of the pause itself: in response to questions from reporters, Department officials pointedly declined to rule out cancelling CMMC altogether at the conclusion of the review. That uncertainty complicates the near-term calculus for contractors deciding whether to continue, defer, or accelerate third-party certification investments, and for prime contractors weighing how to address CMMC in subcontractor flow-downs when the shape of the final program is unknown.[2] Contractors would be well advised to preserve, rather than unwind, the cybersecurity gains they have made—not only because the substantive DFARS 252.204-7012 obligations persist regardless of the certification framework and the Department of Justice continues to announce enforcement actions targeting non-compliance, but also because a mid-review reversal or a modified successor program could reintroduce assessment requirements on short notice.

Finally, and importantly, the enforcement risk that has always run alongside these obligations remains firmly in the background. The Department of Justice continues to devote resources to its Civil Cyber-Fraud Initiative and has pursued alleged non-compliance with contractual cybersecurity requirements—including under DFARS 252.204-7012 and 252.204-7020—as a basis for False Claims Act (FCA) liability. With Phase I self-assessments remaining in force, inaccurate or unsupported self-attestations posted to SPRS present a continuing area of FCA exposure that the suspension of third-party assessment requirements does nothing to diminish, and may arguably heighten as self-assessment becomes, for now, the operative verification mechanism.[1]

We will continue to monitor the CMMC Reform Task Force's review and will report on the Task Force's findings and any successor rulemaking. In the interim, contractors should maintain their existing cybersecurity programs, monitor solicitations and contracts for amendments removing Phase II requirements, and evaluate whether to participate in the RFI before the August 14, 2026 deadline.

Footnotes

[1] This request suggests that the DoW is considering requiring compliance with less than all of the 110 NIST SP 800-171 controls.

[2] Because prime contractors remain responsible for flowing down applicable cybersecurity requirements to subcontractors and suppliers that process, store, or transmit FCI or CUI, the absence of a defined future-state program complicates the drafting and administration of subcontract terms during the review period.

Related Attorneys

David Robbins
Partner
drobbins@jenner.com
+1 202 639 6040

Moshe B. Broder
Partner
mbroder@jenner.com
+1 202 637 6334

Matthew L. Haws
Partner
mhaws@jenner.com
+1 202 639 6065

Related Articles

Department of Defense Marches Forward with CMMC Requirements in Proposed Rule

Related Capabilities

Government Contractor Litigation and Compliance

Stay Informed →