
CLIENT ALERT | July 30, 2026

What Defense Contractors Should Know About DOD's Suspension of CMMC Phase 2

The suspension halts the third-party assessment requirement for defense contractors handling Controlled Unclassified Information (CUI), but cybersecurity obligations and potential FCA exposure remain.

In a July 13, 2026, [memorandum](#) (CMMC Reform Memorandum) and [press release](#), the US Department of Defense (Department of War)¹ suspended Phase 2 of the Cybersecurity Maturity Model Certification (CMMC) program, pausing the requirement that contractors handling CUI obtain third-party assessments by November 10, 2026. DOD also established a CMMC Reform Task Force to conduct a 60-day review of the CMMC program, synthesize industry feedback, and issue recommendations.

Importantly, the suspension of government-required third-party assessments as a prerequisite to obtaining new contracts does not suspend the existing cybersecurity requirements for government contractors. Defense contractors must continue to protect CUI, implement all NIST SP 800-171 Rev. 2 controls to achieve a passing CMMC Level 2 score, and flow down applicable contractual requirements to subcontractors. Self-assessment certifications, Supplier Performance Risk Systems (SPRS) score submission, and other affirmations of compliance remain an area of potential exposure for contractors, particularly in light of the US Department of Justice's (DOJ's) continued use of the False Claims Act (FCA) to enforce cybersecurity requirements pursuant to its Civil Cyber-Fraud Initiative.

For more information on the CMMC program's three-tiered certification framework, self-assessment and third-party assessment requirements, and phased rollout, see this [Client Alert](#).

Background: The CMMC 2.0 Framework

CMMC Phase 2 was originally scheduled to begin on November 10, 2026, and would have required CMMC Third-Party Assessor Organization (C3PAO) assessments for most Level 2 contractors as a condition of contract award. Level 2 covers contractors that process, store, or transmit CUI,² and requires implementation of all 110 NIST SP 800-171 Rev. 2 controls pursuant to Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, with either a self-assessment or C3PAO assessment every three years depending on the solicitation.

Level 3 addresses the most sensitive CUI handled by contractors supporting DOD's highest-priority projects and missions, requiring both a Level 2 (C3PAO) assessment and compliance with 24 additional NIST SP 800-172 requirements verified through a government assessment conducted by the Defense

Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). Although Level 3 (DIBCAC) assessments were not scheduled to become mandatory until Phase 3, which is set to begin one year after the beginning of Phase 2, DOD had discretion to require them earlier for select contracts during Phase 2.

DOD Pauses CMMC Phase 2 and the C3PAO Requirement

The CMMC Reform Memorandum and press release announced an immediate suspension of CMMC Phase 2, pausing the requirement that DOD contractors and subcontractors handling CUI obtain a C3PAO assessment as a condition of contract award. Instead, as explained in the companion implementation memorandum ([Duffey Memorandum](#)), during the period of suspension, "[p]rogram Managers and requiring activities must only include the need for CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement request and requirement documents." The suspension also bars program offices from designating DIBCAC assessments during the review period, alongside C3PAO assessments.³

The suspension similarly halts the case-by-case waiver process that previously allowed DOD to exempt a specific procurement from a CMMC assessment requirement altogether, since no waivers will be granted while program offices remain barred from designating the Level 2 (C3PAO) or Level 3 (DIBCAC) assessments that a waiver would otherwise excuse.⁴

DOD framed the suspension as a way to "maintain a strict security baseline while removing paralyzing costs and keeping innovators and competition growing in the defense supply chain" and "reduce compliance barriers for small and medium sized businesses" in line with Secretary Pete Hegseth's directive.⁵ DOD assigned a CMMC Reform Task Force to conduct a 60-day review of the program, analyze industry feedback, and propose recommendations reflecting "realistic, scalable security measures that prioritize speed to capability and lower barriers for small and non-traditional businesses."⁶

The CMMC Phase 2 suspension is consistent with the Trump administration's broader reassessment of cybersecurity and technology compliance frameworks, including FedRAMP 20x, the General Services Administration's initiative to develop a new cloud-native authorization process designed to be simpler to automate and allow companies to validate the security of their services continuously and efficiently.⁷

The pause also responds to longstanding concerns recognized across government and industry about the burden imposed by CMMC on small defense contractors.⁸ For instance, Kelly Loeffler, the administrator of the US Small Business Administration (SBA), acknowledged that "CMMC compliance was becoming an untenable barrier pushing [small businesses] out of the Defense Industrial Base."⁹

What Has Not Changed for Contractors

Though DOD paused CMMC's rollout, it has not waived or reduced contractors' cybersecurity obligations. The pause does not eliminate contractors' obligation to protect federal data pursuant to Federal Acquisition Regulation (FAR) 52.204-21, or DFARS 252.204-7012 for contractors handling CUI. DOD has confirmed that "[a]ll Phase 1 self-assessment requirements remain firmly in place."¹⁰ DOD program offices may still include CMMC Level 1 (Self) or Level 2 (Self) requirements in procurement documents. DOD

program offices can still mandate that contractors demonstrate CMMC compliance, but only through the self-assessment pathway, not through third-party certification.

Contractors that process, store, or transmit CUI should therefore continue implementing NIST SP 800-171 Rev. 2 controls to achieve a passing CMMC Level 2 score and maintaining CMMC Level 2 self-assessments to ensure eligibility for CMMC-covered contracts. Where DFARS 252.204-7021 applies, contractors must maintain a current CMMC status “for the duration of the contract” and complete annual affirmations of continuous compliance through an “affirming official.”¹¹ Primes and subcontractors will still need to manage flow-down obligations and assurances of compliance, even in the absence of mandatory C3PAO assessments. Contractors handling CUI also remain subject to government audits, typically performed by DIBCAC, to ensure compliance with NIST SP 800-171 requirements where DFARS 252.204-7020 applies.¹²

FCA Risk Remains

DOJ, through its Civil Cyber-Fraud Initiative, increasingly uses the FCA to investigate and prosecute contractors that knowingly misrepresent their cybersecurity compliance.¹³ Defense contractors subject to cybersecurity requirements, including CMMC requirements, may face potential FCA exposure for non-compliance. This risk remains during the suspension of CMMC Phase 2, especially where contractors must certify their own CMMC Level 2 (Self) compliance during the suspension to remain eligible for covered contracts. A false affirmation or overstatement in those affirmations may expose contractors to significant FCA liability and other administrative actions, including contract termination and potential suspension or debarment.

While C3PAO assessments under CMMC Phase 2 or DIBCAC under CMMC Phase 3 may have provided a crucial layer of defense to an allegation that a contractor had knowledge of noncompliance with cybersecurity requirements, pausing Phase 2 could introduce other potential FCA defenses, including materiality defenses. For example, some may view DOD’s suspension of Phase 2 as a signal that the government no longer regards CMMC compliance as material to its contracting and payment decisions, undermining the materiality element of any FCA claim premised on noncompliance with CMMC requirements. While there are likely to be conflicting views on this topic, it remains to be seen how the Phase 2 suspension will impact FCA enforcement actions.

Key Takeaways for Contractors

- **Review DOD solicitation and contract language for CMMC requirements that are now suspended.** Contractors should consider evaluating any active solicitations or existing contracts that include CMMC Level 2 (C3PAO) or Level 3 (DIBCAC) assessment requirements. Under the implementing memorandum, DOD contracting officers are directed to amend active solicitations to explicitly remove those requirements and to modify existing contracts to remove those requirements prior to the next option period or scheduled administrative modification. Contractors who identify suspended requirements in their current agreements may want to proactively engage their contracting officers to confirm the timeline for removal.

- **Continue complying with existing cybersecurity requirements.** The suspension does not amount to a pause in cybersecurity compliance. Though DOD paused the C3PAO requirement, contractors handling CUI remain subject to NIST SP 800-171 Rev. 2 controls and DFARS 252.204-7012 and CMMC Level 2 requirements where applicable. Contractors also remain subject to government audits to validate compliance with NIST SP 800-171 requirements.
- **Review controls related to cybersecurity certifications, affirmations, and submissions.** Contractors should closely review their process for making cybersecurity-related certifications, affirmations, and submissions to the government, prime contractors, or higher-tier subcontractors. For example, contractors should ensure self-assessment scores reported to the government accurately reflect the status of their cybersecurity compliance.
- **Preserve contemporaneous evidence of compliance and remediation.** Now that the third-party assessment requirements are suspended, the burden shifts to contractors to self-assess for compliance. Contractors should maintain contemporaneous documentation showing implemented controls, assessment results, remediation plans, closure of Plan of Action and Milestones (POA&M) items, vulnerability management, incident response activities, and internal approvals for any compliance representation. Robust documentation will be critical to mitigating FCA and related enforcement or audit risk.
- **Determine whether to proceed with an independent assessment during the pause.** Although DOD has paused mandatory C3PAO assessments during the Phase 2 suspension, some contractors may still elect to obtain a C3PAO assessment, readiness review, or other independent evaluation to support customer confidence, strengthen bid positioning, create evidence of good-faith compliance, and strengthen their defense against potential FCA allegations. Entities that have already undergone independent assessments should preserve all supporting documentation and findings, as that record may prove important in responding to future FCA inquiries or other enforcement actions.
- **Flow-down requirements still apply.** Defense contractors remain responsible for flowing down applicable cybersecurity requirements and obtaining appropriate assurances of compliance from subcontractors. Subcontractors that handle CUI should be prepared to provide clear assurances and supporting documentation of their cybersecurity practices to remain competitive in the defense supply chain.
- **Monitor the 60-day review and solicitation language closely.** The CMMC Reform Task Force may recommend changes to the program, but current obligations remain in force unless and until DOD modifies them. Contractors should continue reviewing solicitations, contract clauses, and customer communications for applicable cybersecurity requirements.

This Client Alert was prepared with the assistance of summer associate Olivia Richert.

Contacts

Anne W. Robinson

anne.robinson@lw.com
+1.202.637.2161
Washington, D.C.

Kyle R. Jefcoat

kyle.jefcoat@lw.com
+1.202.637.2152
Washington, D.C.

Dean W. Baxtreser

dean.baxtreser@lw.com
+1.202.637.2110
Washington, D.C.

Morgan L. Maddoux

morgan.maddoux@lw.com
+1.505.270.0489
Washington, D.C.

Drew Diachenko

drew.diachenko@lw.com
+1.415.395.8086
San Francisco

Chris Caulder

chris.caulder@lw.com
+1.202.637.2297
Washington, D.C.

Ysa Gomez-Gonzalez

ysa.gomez-gonzalez@lw.com
+1.424.653.5626
Los Angeles

Pascal Jakowec

pascal.jakowec@lw.com
+1.213.891.8397
Los Angeles

This publication is produced by Latham & Watkins as a news reporting service to clients and other friends.

The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. See our [Attorney Advertising and Terms of Use](#).

Endnotes

¹ <https://www.whitehouse.gov/presidential-actions/2025/09/restoring-the-united-states-department-of-war/>.

² Per [32 CFR § 2002.4](#), CUI is information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that requires safeguarding or dissemination controls under applicable law, regulation, or government-wide policy. Within [the DOD CUI Program Organizational Index](#)'s Defense grouping, one example category is Controlled Technical Information (CTI), which covers technical data with military or space applications, such as engineering drawings, test reports, and cybersecurity plans.

³ "Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements" available here: <https://dodcio.defense.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf>.

⁴ *Id.*

⁵ "Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements" available here: <https://www.war.gov/News/Releases/Release/Article/4542329/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/>.

⁶ *Id.*

⁷ Although DOD's memorandum and press release do not specify AI as the reason for the changes to CMMC, the decision to pause CMMC Phase 2 aligns with this administration's general policy approach to accelerate domestic AI development and deployment through de-regulation. On December 11, 2025, the administration issued an [executive order](#) titled "Ensuring a National Policy Framework for Artificial Intelligence," stating: "It is the policy of the United States to sustain and enhance the United States' global AI dominance through a minimally burdensome national policy framework for AI." The administration has also described its [AI Action Plan](#) as removing "onerous Federal regulations that hinder AI development and deployment," as well as seeking input from industry on which federal rules and regulations to remove.

⁸ In the CMMC Reform Memo, DOD CIO Kirsten A. Davies stated: "The combination of prohibitive compliance costs, severe shortages in third-party assessment capacity, and complex regulatory timelines is actively forcing innovative new entrants and

small businesses to opt out of [DOD] contracts and freezing critical suppliers out of the market.” In addition, the SBA acknowledged that Phase 2 would have required more than 120,000 small businesses in the defense industrial base to seek compliance “through a cost-prohibitive system supported by only about 100 approved assessors.” The SBA estimated that small firms would pay \$593,800 per C3PAO certification and \$388,600 for self-assessments. “SBA Commends U.S. Department of War’s Suspension of CMMC Phase II for Small Defense Contractors” available here:

<https://www.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors>.

⁹ “SBA Commends U.S. Department of War’s Suspension of CMMC Phase II for Small Defense Contractors” available here:

<https://www.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors>.

¹⁰ “Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements” available here:

<https://www.war.gov/News/Releases/Release/Article/4542329/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/>.

¹¹ DFARS 252.204-7021 available here: <https://www.acquisition.gov/dfars/252.204-7021-contractor-compliance-cybersecurity-maturity-model-certification-level-requirements>.

¹² Effective February 1, 2026, DFARS 252.204-7020 has been renumbered to DFARS 252.240-7997 under DOD Class Deviation 2026-O0025, available here: https://www.acq.osd.mil/dpap/dars/classdev/DFARS_RFO/Part-240/2026-O0025_TAB_A_Deviation_Memo_DFARS_240.pdf.

¹³ On January 16, 2026, DOJ announced that False Claims Act settlements and judgments exceeded \$6.8 billion in the fiscal year ending Sept. 30, 2025, noting that “[t]he Department also continued to advance cases holding government contractors and grantees accountable when they knowingly violate applicable cybersecurity requirements.” DOJ Press Release: “False Claims Act Settlements and Judgments Exceed \$6.8B in Fiscal Year 2025” available here: <https://www.justice.gov/opa/pr/false-claims-act-settlements-and-judgments-exceed-68b-fiscal-year-2025>.