NCMBC WHITE PAPER

The CMMC Phase 2 Suspension:

What Changed, What Did Not, and What Defense Contractors Should Do Now

Tim Malone

Regional Program Manager, North Carolina Military Business Center

E: malonet@ncmbc.us P: 910-362-7175

July 29, 2026

This white paper is provided for general informational purposes only and does not constitute legal advice. Each firm's actual obligations are established by the clauses in its own contracts and subcontracts. The regulatory situation described here is evolving; all statements reflect guidance in effect as of July 29, 2026, while the report of the CMMC Reform Task Force remained pending. Readers should verify current status against the primary sources cited before acting.

Executive Summary

On July 13, 2026, the Department of War (DoW) announced the immediate suspension of Phase 2 of the Cybersecurity Maturity Model Certification (CMMC) program, which had been scheduled to take effect on November 10, 2026, along with all pending and future CMMC implementation milestones. [1, 2, 3] The action removes, for the duration of a formal review, the Department's requirement that contractors obtain third-party or government-led certification assessments as a condition of contract award. It does not remove any underlying obligation to protect federal information.

The distinction matters because the suspension arrived by memorandum, not by regulation. The two July 13 documents, a policy memorandum from the DoW Chief Information Officer and an implementation memorandum from the Office of the Under Secretary for Acquisition and Sustainment, were released under publication case 26-P-1023. [1, 6] No Federal Register action accompanied them. The CMMC Program rule at 32 CFR Part 170 and the acquisition rule implementing it, including DFARS clause 252.204-7021, remain in force exactly as written. [6, 9] What has stopped is the Department's exercise of its discretion to require the higher assessment types, not the regulatory framework itself.

During the suspension, program managers and requiring activities may designate only CMMC Level 1 (Self) or Level 2 (Self) in requirements documents. Level 2 (C3PAO) and Level 3 (DIBCAC) may not be designated, and no CMMC waivers will be granted during the review period. [1] The Department has directed that active solicitations containing the suspended requirements be amended as soon as practicable, and that existing contracts be modified before the next option exercise or during the next scheduled administrative modification. [1, 3]

Everything else stands. Contractors handling Controlled Unclassified Information (CUI) remain bound by DFARS 252.204-7012 to implement NIST SP 800-171 Revision 2, to report cyber incidents to the Department within 72 hours, and to flow those requirements down to subcontractors. Phase 1 self-assessment requirements, Supplier Performance Risk System (SPRS) scores, and annual affirmations of compliance remain fully in effect, and the Department will continue select government-led assessments. [1, 3, 8] Because a signed SPRS affirmation is a representation to the government, the practical enforcement weight of the program now rests more heavily, not less, on the accuracy of self-assessments.

A CMMC Reform Task Force has been established to conduct a top-to-bottom review of the program and deliver recommendations to the DoW CIO within 60 days, placing its report in mid-September 2026. A public Request for Information closed the comment window at 12:00 p.m. Eastern on August 14, 2026. [5, 11, 12, 14] This paper summarizes what the suspension changed, the cost and capacity data that prompted it, the direction the review may take, the parallel movement of the proposed FAR CUI rule toward NIST SP 800-171 Revision 3, and the practical steps contractors in three different postures should take while the outcome is pending.

1. Background: How CMMC Reached Phase 2

CMMC exists because Congress required it. Section 1648 of the National Defense Authorization Act for Fiscal Year 2020 directed the Department to develop a cybersecurity framework for the defense industrial base, and both the program rule and the acquisition rule identify that statute as the authority they implement. [9, 24, 25] The program's premise dates to earlier findings, including a 2019 Department Inspector General report documenting widespread noncompliance with the safeguarding requirements that DFARS 252.204-7012 had imposed since 2017.

The modern program took final regulatory form in two stages. The CMMC Program rule, published at 32 CFR Part 170 in October 2024 and effective that December, defined the three CMMC levels, the assessment types (self-assessment, certification by a CMMC Third-Party Assessment Organization or C3PAO, and assessment by the Defense Industrial Base Cybersecurity Assessment Center or DIBCAC), and the program's phased implementation plan. [24, 25] The companion acquisition rule amending the DFARS took effect in November 2025, allowing contracting officers to place CMMC requirements in solicitations through clause 252.204-7021. [5, 24]

Implementation was phased deliberately. Phase 1, which began with the acquisition rule in November 2025, required self-assessments: Level 1 for contractors handling Federal Contract Information (FCI) under FAR 52.204-21, and Level 2 self-assessment for contractors handling CUI, each accompanied by a score posted to SPRS and an annual affirmation of continuing compliance. [1, 3] Phase 2, scheduled for November 10, 2026, would have permitted requiring activities to demand certification assessments, principally Level 2 C3PAO certification, as a condition of award across contracts involving CUI. Department officials estimated that roughly 80,000 companies would eventually fall under the third-party assessment requirement. [5] Phase 3 was scheduled for November 2027, with full implementation planned for 2028. [8]

2. The July 13, 2026 Suspension: Precisely What Changed

The implementation memorandum is specific, and its language rewards close reading. Four operative provisions define the suspension:

- **Assessment designations restricted.** During the suspension, program managers and requiring activities must include only CMMC Level 1 (Self) or Level 2 (Self) in procurement requests and requirements documents, and may not designate Level 2 (C3PAO) or Level 3 (DIBCAC). [1]
- **Active solicitations amended.** Where a requirements package included a Level 2 (C3PAO) or Level 3 (DIBCAC) requirement, requiring activities must initiate amendments removing it, and the contracting officer must issue a corresponding solicitation amendment as soon as practicable. [1]
- **Existing contracts modified.** Contracting officers are directed to remove the suspended requirements from existing contracts by modification prior to exercising the next option period or during the next scheduled administrative modification. [1]
- **Waivers suspended.** Because the higher assessment types cannot be designated at all, no CMMC waivers will be granted during the review. [1]

The memorandum then states what continues: the Department will enforce baseline compliance with NIST SP 800-171 Revision 2 through Level 1 and Level 2 self-assessment and through select government-led assessments, and the requirements of DFARS 252.204-7012 remain in effect. [1]

2.1 A suspension by memorandum, not by rule

Legal analysts noted immediately that the suspension is an exercise of administrative discretion rather than a change in law. No Federal Register document was issued, 32 CFR Part 170 is unamended, no DFARS class deviation has been published, and clause 252.204-7021 remains in force as written. [6] Until a modification actually reaches a given contract, the clause in that contract remains the contract, and DFARS 204.7503(c) continues to bar exercise of an option unless the contractor's required CMMC status is current in SPRS. [6] The practical consequence for contractors is direct: where a suspended requirement sits in an active contract or solicitation, request the modification or amendment in writing rather than assuming it.

2.2 What remains fully in force

A reader who takes one thing from this paper should take this list. The following obligations were not suspended and continue to apply:

Obligation	Continuing effect
DFARS 252.204-7012	Safeguard covered defense information by implementing NIST SP 800-171 Rev 2; report cyber incidents to DIBNet within 72 hours; flow the clause down to subcontractors handling covered defense information [1, 3, 6]
CMMC Phase 1 self-assessments	Level 1 and Level 2 self-assessment requirements, SPRS score submission, and annual affirmations remain firmly in place [3]
FAR 52.204-21	The fifteen basic safeguarding requirements for Federal Contract Information continue to apply to every contractor and subcontractor whose systems hold or transmit FCI [1]
Government-led assessments	DIBCAC and other government-led reviews continue during the suspension at the Department's discretion [1, 8]
Cloud and export-control obligations	FedRAMP Moderate (or equivalent) expectations for CUI in cloud services and ITAR/EAR data controls are unaffected by the CMMC action [9]
Prime contractor flowdowns	Certification requirements that prime contractors have written into their own subcontracts are private contractual terms; the government's pause does not amend them [18]

3. What Prompted the Suspension

The Department's stated rationale is economic. The Small Business Administration, which publicly endorsed the suspension, estimated total compliance costs of approximately $593,800 per CMMC certification for small firms requiring third-party assessment and approximately $388,600 for firms eligible for self-assessment, and observed that Phase 2 as scheduled would have required more than 120,000 small businesses in the defense industrial base to pursue compliance through a system supported by only about 100 approved assessment organizations. [4] DoW CIO Kirsten Davies cited SBA data suggesting that future CMMC phases could impose more than $7 billion in annual costs on small and mid-sized businesses, remarking that “the math just simply doesn’t math.” [7]

Independent oversight had reached similar conclusions. A March 2026 Government Accountability Office report, GAO-26-107955, warned that the requirements could push small businesses out of the defense industrial base. [7] The suspension was framed as an implementation of Secretary Hegseth's acquisition reform initiatives, and the CIO's policy memorandum, titled “Removing Barriers to Defense Industrial Base Expansion,” reflects the Department's concern that the program was slowing procurement by imposing front-end costs some contractors could not absorb. [3, 13] The Department also stated that it had found unnecessary duplication within the existing cybersecurity requirements framework and intends the review to streamline the regulations. [15]

Under Secretary Michael Duffey summarized the policy position: “We’re not relaxing the standards by any means.” The Department expects continued adherence to the NIST standards; what it is removing, in his framing, is the bureaucracy of the third-party assessment. [9] Department officials have described the intended emphasis as tangible cyber hygiene rather than certification paperwork. [5]

Congress, notably, had been moving in a complementary rather than contradictory direction on cost. The Senate Armed Services Committee's fiscal year 2027 defense authorization bill includes a CMMC grant program, capped at $50 million in total and $100,000 per grant, restricted to offsetting the direct costs of a Level 2 third-party assessment, prioritizing firms that have never held a Department contract, and requiring the program to stand up by July 1, 2027. [23] Whether that provision survives conference in a post-suspension environment is unknown, but its existence indicates that the legislature regarded the assessment cost problem as one to subsidize rather than a reason to abandon the program.

4. The 60-Day Review and What May Follow

The CIO's memorandum establishes a CMMC Reform Task Force to conduct a comprehensive top-to-bottom review of the program. The task force serves as the central hub for synthesizing industry feedback from a public Request for Information on compliance challenges, and is charged with recommending realistic, scalable security measures that prioritize speed to capability and lower barriers for small and non-traditional businesses, delivering its final report to the DoW CIO within 60 days. [11] The task force convened for the first time within days of the announcement. [5] The RFI comment window closed at 12:00 p.m. Eastern on Friday, August 14, 2026, and the report is due in mid-September 2026. [12, 14]

The RFI's questions are the best available indication of direction. The Department sought industry perspectives on the burden of compliance, on the commercial cybersecurity solutions companies already use, on how the Department might better recognize or accept those solutions within a compliance or risk framework, and on leveraging and optimizing self-assessments. [5, 11] Read together, those questions suggest a review weighing whether verification can rest on self-assessment, government-led spot checks, and recognition of existing commercial certifications rather than on a bespoke third-party assessment industry.

4.1 Two directions, honestly weighed

Because the task force report was pending when this paper was written, the responsible framing is a set of signals rather than a prediction. The considerations below capture the strongest case for each of the two broad outcomes.

Consideration	Case that the framework holds	Case that the framework is rebuilt
The legal floor	Section 1648 of the FY20 NDAA requires a supply-chain cybersecurity framework to exist; retaining Level 1 and Level 2 self-assessment already satisfies it [10, 24]	The statute requires a framework, not this framework; Congress set the outcome and left the design open [10]
The task force charter	The memorandum directs a review and interim relief, the usual precursor to retaining what works minus its most expensive element	The task force is charged with redesigning the Department's supply-chain cybersecurity approach and recommending a reformed framework [11]
Speed and machinery	Sixty days is enough time to decide what to stop doing, not to design, cost, and socialize a replacement	Sixty days is enough to pick a direction; the build-out follows the report rather than preceding it [5]
Enforcement economics	Self-assessment, SPRS scoring, and False Claims Act exposure already exist and cost the government little	Self-attestation without verification is the failure mode earlier oversight identified; removing audits implies a different verification model
Precedent	Every prior CMMC delay ended with the program resuming roughly as written; timelines slipped while the framework held	The last top-to-bottom review turned CMMC 1.0 into CMMC 2.0: five levels became three, maturity processes were deleted, and self-assessment was reintroduced

Three observable tells will resolve the question after the report issues. First, whether anything reaches the Federal Register: recommendations implemented only by memorandum leave the codified rules saying what they now say, while a proposed rule or class deviation signals durable change. Both the 32 CFR program rule and the acquisition rule remain in effect and cannot lawfully be rewritten without proper rulemaking.[9] Second, whether NIST SP 800-171 survives by name as the technical anchor. Third, what happens to the C3PAO ecosystem: continuation with a narrowed critical-programs role means the audit model is being scoped down, while allowing accreditation to wither means it is being replaced. The outcome may also be a hybrid, in which the standard survives while the verification layer is restructured around self-assessment, government spot checks, and recognition of commercial certifications.

5. "Brilliant at the Basics"

Alongside the suspension, the DoW CIO launched a campaign titled "Brilliant at the Basics," described as an initiative dedicated to helping small, mid-sized, and non-traditional defense industrial base companies secure their networks and protect sensitive Department information. [2] The campaign publishes two top-ten lists of best practices, one for information technology environments and one for operational technology (OT), together with a curated set of free resources from the Department, CISA, NIST, and the NSA Cybersecurity Collaboration Center. [2]

The IT list emphasizes phishing-resistant multi-factor authentication, comprehensive asset inventory, reduction of technical debt, a flexible and interoperable technology stack, logical segmentation to limit lateral movement, risk-based vulnerability management, integration of security early in the development lifecycle, secure adoption of artificial intelligence including an explicit prohibition on placing sensitive Department data into public commercial AI systems, resilient and immutable backup architecture with tested restoration, and continuous technical workforce development. [2] The OT list addresses identity and access control, validated asset inventory, strict network segmentation, OT-specific incident response, compensating controls for unpatchable equipment, restricted remote access, continuous monitoring, system resiliency, supply chain security, and formal change review. For engineering and construction firms, whose environments include building automation, plant controls, and equipment telematics, the existence of a dedicated OT list is itself notable.

Two characterizations should be kept in balance. First, the campaign is guidance, not a compliance standard: it does not replace what is written into any contract, and the page carries its own disclaimer to that effect. [2, 18] Second, it is not simply an abridged CMMC. Several of its priorities, including technical debt reduction, vendor-lock-in avoidance, secure AI adoption, shift-left development security, and tested immutable backups, have no direct analog among the 110 requirements of NIST SP 800-171 Revision 2, while the documentation apparatus that drives much of the cost of Level 2 compliance, such as the system security plan and plan of action process, is conspicuously absent from it. The campaign is best read as a statement of philosophy, outcome-based hygiene over control-based paperwork, and as a plausible preview of the direction the Reform Task Force has been asked to chart. [5, 8]

6. NIST SP 800-171 Revision 3 and the Proposed FAR CUI Rule

A frequent question is whether the suspension accelerates or delays the transition to NIST SP 800-171 Revision 3. In the near term it does neither: it re-confirms Revision 2. NIST published Revision 3 in May 2024, reorganizing the standard into 97 requirements across 17 families, but the Department issued DFARS Class Deviation 2024-O0013 that same month, expressly requiring contractors subject to DFARS 252.204-7012 to continue complying with Revision 2, and the CMMC program rule is written against Revision 2. [15, 16] The July 13 implementation memorandum reiterates Revision 2 as the enforced interim baseline. [1] Before Revision 3 can anchor the defense program, the Department must update DFARS 252.204-7012 through rulemaking, align 32 CFR Part 170, publish revised assessment guides, and provide a transition period; the Department released its organization-defined parameters for Revision 3 in April

2025, a signal of active preparation, and observers place realistic adoption in the late 2026 to 2027 window at the earliest, a timeline now further subject to the task force's recommendations. [15, 17]

The more consequential movement is occurring outside the Department. On June 23, 2026, the FAR Council issued a revised proposed rule governing Controlled Unclassified Information across the entire federal government, part of the broader FAR overhaul implementing Executive Order 14275. As proposed, the rule would require contractor information systems handling CUI to meet NIST SP 800-171 Revision 3, would subject a limited set of contractors handling CUI associated with critical programs or high-value assets to enhanced requirements from NIST SP 800-172, would impose 72-hour CUI incident reporting, would require agencies to identify the CUI involved in a contract on a standard form incorporated into the solicitation, and would flow safeguarding requirements down to subcontractors at all tiers that access covered CUI. [19, 20, 21] The comment period closed on July 23, 2026. [19]

The juxtaposition deserves emphasis. The Department of War is pausing third-party audits against Revision 2 at the same time the FAR Council proposes Revision 3 for every federal contractor handling CUI. A firm holding both a defense contract and a civilian-agency contract could, if the proposed rule finalizes in its current form, find itself measured against two different revisions of the same standard depending on which agency issued the contract. [22] The proposed FAR rule is not yet in effect and may change before finalization, but it forecloses any reading of the July 13 action as a general federal retreat from CUI safeguarding. It also means that security investments aligned to NIST SP 800-171 retain their value under every plausible outcome of the Department's review.

7. Flowdown: How Far the Requirements Reach

For general contractors and their supply chains, flowdown is often the decisive question, and the answer follows the data rather than the organizational chart. DFARS 252.204-7012 flows down to subcontractors at every tier whose performance involves covered defense information or operationally critical support, with commercially available off-the-shelf items as the principal exemption, and the clause's 72-hour incident-reporting and safeguarding obligations travel with it unaltered. [6] Where CMMC requirements are included in a contract under clause 252.204-7021, they likewise reach subcontractors at all tiers whose systems process, store, or transmit FCI or CUI, with the required level determined by the information involved: FCI alone corresponds to Level 1, while CUI requires at least Level 2. A third-tier detailer or testing laboratory that receives controlled drawings is within the flowdown; a subcontractor that never receives federal information is not.

The suspension adds a wrinkle that will surprise many subcontractors: the government paused its requirements, but prime contractors did not necessarily pause theirs. Many primes had begun flowing certification requirements into their subcontracts ahead of the November deadline, independent of the federal rollout. They are under no obligation to relax supply-chain requirements because the Department paused Phase 2, some may hold firm on requirements already communicated, and subcontractors should confirm their prime's position directly, in writing, rather than assume the pause applies to their agreement. [18] Prime contractors, for their part, should assess whether subcontract terms referencing Phase 2 milestones require modification or formal communication to supply-chain partners, and offerors

should evaluate whether pending proposals reference requirements that are now inapplicable and seek direction from the contracting officer. [14]

8. Practical Guidance by Contractor Posture

The most useful organizing principle for spending decisions during the review period is the distinction between durable and perishable investment. Durable spending buys actual security and remains contractually required under DFARS 252.204-7012 regardless of the task force outcome. Perishable spending buys preparation for a specific audit event that may not occur on the previously assumed schedule.

Durable (continue)	Perishable (pause and reassess)
Multi-factor authentication, resilient backups, network segmentation, logging and monitoring, endpoint protection	C3PAO scheduling deposits and assessor logistics
Enclave design and scope-reduction work that shrinks the assessment boundary	Mock assessments and readiness rehearsals keyed to a specific assessor's methodology
System security plan and plan of action, which are requirements of NIST SP 800-171 itself (3.12.2 and 3.12.4), not audit artifacts	Evidence packaging produced solely for certification presentation
Accurate SPRS scoring, annual affirmations, and incident-response readiness including DIBNet reporting	Headcount or premium retainers acquired purely to survive an audit date

8.1 Firms that have not started

The first step is not selecting a level; it is determining what information the firm's systems actually hold. A contractor whose systems touch only Federal Contract Information sits in FAR 52.204-21 territory, mirrored by CMMC Level 1 self-assessment, a requirement of Phase 1 that the suspension did not touch. A contractor handling CUI owes implementation of NIST SP 800-171 Revision 2 under DFARS 252.204-7012, an obligation that predates CMMC and survives it; the suspension removed the auditor, not the requirement. [1, 3] The present period, free of a November deadline and the assessor scheduling scramble that was building toward it, is the lowest-pressure window in several years in which to begin. The failure mode to avoid is treating the suspension as cancellation, doing nothing, and then signing an SPRS affirmation anyway; Section 9 describes what that can cost.

8.2 Firms in mid-implementation

Continue, but re-sequence. Everything in the durable column above proceeds; audit-specific spending can pause pending the September report. The time recovered is best invested in scope reduction, because a smaller compliance boundary lowers cost under every scenario the task force could select and under the

proposed FAR CUI rule besides. Two administrative actions carry particular urgency: obtaining the prime contractor's position on its own flowdown requirements in writing, since those requirements did not pause with the government's [18], and reviewing any multi-year service or platform agreements sized to the former November deadline for re-phasing options, a contract-terms question on which firms should consult their own agreements and, where warranted, counsel.

8.3 Firms that have scheduled or paid for an assessment

Four questions frame the decision. First, where did the money actually go: for most firms the assessment fee is the minority of total program spend, with the majority in readiness work that DFARS 252.204-7012 required in any event and that retains its value. Second, is a prime contractually requiring the certification: if so, the Department's pause is largely irrelevant and finishing is usually the right answer. Third, what do the C3PAO's own terms provide regarding deferral, credit, or refund: these vary by agreement and should be obtained in writing before any decision. Fourth, for firms already holding a conditional certification status, the 180-day close-out period attached to that status under the program rule [24] is a matter to raise promptly with the assessor and the contracting officer rather than allow to lapse silently.

One uncertainty must be stated plainly rather than smoothed over: whether a reformed program would grandfather certifications already earned is unknown, and any assurance on the point is opinion rather than fact. What can be said without qualification is that completed certifications remain valid tokens in SPRS, that they continue to function as a competitive differentiator with primes that are holding firm on their own requirements, and that the security posture and documentation underlying a certification retain their value regardless of the certificate's future. [18]

9. The Enforcement Risk That Did Not Pause

Because the suspension shifts the program's weight onto self-assessment, the accuracy of those self-assessments becomes the central compliance exposure. Every SPRS score and every annual affirmation is a signed representation to the government, and the False Claims Act attaches to representations. In one recent matter, a contractor reported a perfect SPRS score of 110 while a government-led review of the same environment scored it at negative 170; the resulting False Claims Act settlement cost the contractor $507,000. [8] Government-led assessments continue through the suspension. [1, 8] Firms should treat the review period as an opportunity to make their posture and their paperwork agree, not as a holiday from either.

10. Conclusion: Three Questions That Decide It

Policy developments set the ceiling of what the government may require; a firm's actual obligations are set by the clauses in its contracts and subcontracts. Accordingly, the analysis above reduces, for any individual firm, to three questions. First, what information does each contract place on the firm's systems: FCI, CUI, or neither. That single determination drives the applicable level, the cost, and the timeline. Second, what does each prime's subcontract require, and has the prime's position changed since July 13.

Third, what does the clause in each contract currently say, and has the contracting officer issued the directed amendment or modification yet.

The Cybersecurity Maturity Model Certification program is suspended in part and under review in whole, but the statutory mandate behind it stands, the safeguarding obligations beneath it are untouched, and the government-wide regulatory current continues to run toward NIST SP 800-171 rather than away from it. Contractors that continue implementing the standard at a sustainable pace, keep their SPRS representations accurate, and engage their primes and contracting officers in writing will be well positioned under any framework the September report produces.

The North Carolina Military Business Center provides no-cost technical assistance to North Carolina businesses navigating these requirements, including scoping, self-assessment, and implementation planning. Firms with questions about their specific posture are encouraged to contact the author.

References

[1] Department of War, Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification Procedures" (implementation attachment to CIO memorandum), publication case 26-P-1023, July 13, 2026. *https://dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf*

[2] Department of War Chief Information Officer, "Brilliant at the Basics" campaign page (IT and OT top-ten best practices and resources). *https://dowcio.war.gov/BrilliantBasics/*

[3] Crowell & Moring LLP, "DoW Suspends CMMC Phase II Requirements 2026: 60-Day Reform Review, DFARS Obligations & Contractor Action Steps," July 2026. *https://www.crowell.com/en/insights/client-alerts/department-of-war-immediately-suspends-cmmc-phase-ii-requirements-launches-60-day-reform-review*

[4] U.S. Small Business Administration, "SBA Commends U.S. Department of War's Suspension of CMMC Phase II for Small Defense Contractors," July 13, 2026. *https://www.sba.gov/article/2026/07/13/sba-commends-us-department-wars-suspension-cmmc-phase-ii-small-defense-contractors*

[5] Federal News Network, "Pentagon suspends CMMC phase two requirements, launches review of program," July 2026; DefenseScoop, "Pentagon task force to review CMMC hits the ground running," July 17, 2026. *https://federalnewsnetwork.com/cybersecurity/2026/07/pentagon-suspends-cmmc-phase-two-requirements-launches-review-of-program/*

[6] Government Contracts Law, "DoD Suspends CMMC Phase 2: What Happened, What It Means, and What Nobody Is Telling You," July 2026. *https://www.governmentcontractslaw.com/2026/07/dod-suspends-cmmc-phase-2-what-happened-what-it-means-and-what-nobody-is-telling-you/*

[7] ITSecOps, "CMMC Phase 2 Suspended: What Still Applies," updated July 2026 (citing DoW CIO Kirsten A. Davies and GAO-26-107955). *https://itsecops.cloud/cmmc-phase-2-suspended/*

[8] A-LIGN, "What the CMMC Phase II Suspension Means for Defense Contractors," July 2026. *https://www.a-lign.com/articles/cmmc-phase-ii-suspension*

[9] Summit 7, "CMMC Phase 2 Suspended with 60 Day Review. What Happens Next?," July 2026 (including USD(A&S) Michael Duffey remarks). *https://summit7.us/blog/cmmc-phase-2-suspended-with-60-day-review-what-happens-next*

[10] Summit 7, "Is CMMC Going Away? What the DoD Is Actually Saying" (statutory basis under Section 1648, FY20 NDAA), December 2025. *https://summit7.us/blog/is-cmmc-going-away*

[11] Industrial Cyber, "Department of War suspends CMMC Phase II, launches 60-day review to reduce compliance burden on defense contractors," July 2026. *https://industrialcyber.co/threats-attacks/department-of-war-suspends-cmmc-phase-ii-launches-60-day-review-to-reduce-compliance-burden-on-defense-contractors/*

[12] SBA Office of Advocacy, "DoW Requests Information for CMMC Reform Task Force," July 20, 2026 (RFI deadline and submission instructions). *https://advocacy.sba.gov/2026/07/20/dow-requests-information-for-cmmc-reform-task-force/*

[13] Greenberg Traurig LLP, "DoD Suspends CMMC Deadlines and Seeks to Reassess Requirements," July 2026. *https://www.gtlaw.com/en/insights/2026/7/dod-suspends-cmmc-deadlines-and-seeks-to-reassess-requirements*

[14] McGuireWoods LLP (Subject to Inquiry), "DoW Suspends CMMC Phase II Requirements – Launches 60-Day Review," July 2026. *https://www.subjecttoinquiry.com/2026/07/dow-suspends-cmmc-phase-ii-requirements-launches-60-day-review/*

[15] Layer 8 Consulting, "NIST 800-171 Rev 3: What Changed and What It Means for CMMC," February 2026 (Class Deviation 2024-O0013; Rev 3 adoption prerequisites and timeline; April 2025 ODP release). ArentFox Schiff, "CMMC Reform Task Force RFI," July 2026 (duplication finding). *https://layer8consulting.ai/blog/nist-800-171-rev-3*

[16] Secureframe, "NIST 800-171 Rev 2 vs Rev 3: What Changed and What It Means for CMMC," April 2026. *https://secureframe.com/blog/nist-800-171-rev2-vs-rev3*

[17] ISI Defense, "NIST 800-171 Rev 2 vs. Rev 3: What Defense Contractors Need to Know," May 2026 (2026 Unified Agenda rulemaking status). *https://isidefense.com/blog/nist-800-171-rev-2-vs.-rev-3-what-defense-contractors-need-to-know*

[18] ISI Defense, "CMMC Phase II Is Paused, Not Canceled: What Defense Contractors Need to Know," July 2026 (prime flowdown behavior; Brilliant at the Basics characterization). *https://isidefense.com/blog/cmmc-phase-2-is-paused-not-canceled-what-defense-contractors-need-to-know*

[19] Hunton Andrews Kurth LLP, "FAR Council Releases Updated CUI Proposed Rule as Part of the Revolutionary FAR Overhaul," June 2026. *https://www.hunton.com/government-contracts-intelligence-briefing/far-council-releases-updated-cui-proposed-rule-as-part-of-the-revolutionary-far-overhaul*

[20] Wiley Rein LLP, "FAR Council Proposes Revised CUI Framework as Part of Revolutionary FAR Overhaul," June 2026. *https://www.wiley.law/alert-FAR-Council-Proposes-Revised-CUI-Framework-as-Part-of-Revolutionary-FAR-Overhaul-With-Important-Guidance-and-Clarifications*

[21] Skadden, Arps, Slate, Meagher & Flom LLP, "Big Changes Coming for Government Contractors: Proposed FAR CUI and DoW FOCI Rules," June 2026. *https://www.skadden.com/insights/publications/2026/06/big-changes-coming-for-government-contractors*

[22] Mayer Brown LLP, "FAR Council Proposes Revised CUI Safeguarding and Incident-Reporting Framework, While DoW Pauses CMMC Implementation," July 2026. *https://www.mayerbrown.com/en/insights/publications/2026/07/far-council-proposes-revised-cui-safeguarding-and-incident-reporting-framework-while-dow-pauses-cmmc-implementation*

[23] Federal News Network, "Senate NDAA proposes CMMC grant program," June 2026. *https://federalnewsnetwork.com/technology-main/2026/06/senate-ndaa-proposes-cmmc-grant-program/*

[24] White & Case LLP, "Department of Defense releases final DFARS rule implementing Cybersecurity Maturity Model Certification (CMMC) requirements," September 2025. *https://www.whitecase.com/insight-alert/department-defense-releases-final-dfars-rule-implementing-cybersecurity-maturity*

[25] BDO USA, "Defense Contractors Face a New Reality: The Final 48 CFR Rule is Bringing CMMC into Federal Acquisition," October 2025 (Section 1648(c)(2) implementation; 32 CFR Part 170 finalization). *https://www.bdo.com/insights/advisory/defense-contractors-new-reality-the-final-48-cfr-rule-is-bringing-cmmc-into-federal-acquisition*

Primary regulatory texts referenced throughout: 32 CFR Part 170 (CMMC Program); DFARS 252.204-7012, 252.204-7019/-7020, and 252.204-7021; DFARS 204.7503(c); FAR 52.204-21; NIST SP 800-171 Revisions 2 and 3; NIST SP 800-172; Section 1648, National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92).