Can You Subcontract Without CMMC Certification?

What the Phased Rollout Actually Means for Defense Subcontractors

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

The Short Answer Is Not a Simple One

The question comes up constantly among defense subcontractors: can we continue to win and perform on subcontracts without holding a CMMC certification? The answer depends on when the subcontract is awarded, what information flows down from the prime, and which phase of the CMMC rollout applies at the time of award. There is no single yes or no answer that holds across all circumstances, and subcontractors who treat the question as binary are likely to misjudge their exposure.

This paper walks through the regulatory mechanics that govern subcontractor CMMC obligations, explains how the phased implementation schedule affects what is required and when, and addresses the practical reality that many prime contractors are imposing requirements ahead of the formal mandate. The goal is to give subcontractors a clear, regulation-grounded understanding of where they stand today and what they need to be prepared for over the next twelve months.

How CMMC Requirements Reach the Subcontractor

CMMC requirements do not apply to every company in the defense supply chain by default. They apply when a prime contractor is required by the terms of its contract to flow down CMMC obligations to subcontractors who will process, store, or transmit Federal Contract Information or Controlled Unclassified Information on their own information systems.

The governing mechanism is DFARS clause 252.204-7021, which requires the prime contractor to consult 32 CFR 170.23 and flow down the correct CMMC level to subcontracts and other contractual instruments. The clause further requires that, prior to awarding a subcontract, the prime must ensure the subcontractor has a current CMMC certificate or CMMC status at the level appropriate for the information being flowed down. Subcontracts exclusively for commercially available off-the-shelf items are excluded from this requirement.

The determination of what CMMC level applies to a given subcontractor is based on the type of information the subcontractor will handle. If the subcontractor will process, store, or transmit only FCI, Level 1 (self-assessed) applies. If CUI is involved, Level 2 applies, with the assessment type determined by the solicitation. If no FCI or CUI flows down to the subcontractor, no CMMC requirement attaches to that subcontract.

This means that a subcontractor's CMMC obligation is not determined by their own business profile or the nature of their work in general terms. It is determined contract by contract, based on what information the prime needs to share with them to perform the work.

Phase 1: Where Subcontractors Stand Today

Phase 1 of the CMMC rollout began on November 10, 2025. During Phase 1, contracting officers began including CMMC Level 1 and Level 2 self-assessment requirements in applicable solicitations as a condition of award. The Department of Defense retains discretion to require Level 2 C3PAO certification during Phase 1 for contracts it designates as higher priority, but the default requirement for most Level 2 contracts in this phase is a self-assessment.

For subcontractors, this means that the CMMC obligation they face today is most likely a self-assessment requirement. If the prime contract was awarded after November 10, 2025 and includes DFARS 252.204-7021, the prime is required to flow down the appropriate CMMC level. A subcontractor handling CUI under such a contract would need a Level 2 self-assessment score posted in the Supplier Performance Risk System, along with an annual affirmation of continuous compliance by a senior official.

The practical implication is that subcontractors who have not completed a self-assessment and posted their SPRS score are already at risk of being unable to receive new subcontract awards under contracts that carry the CMMC clause. This is not a future obligation. It is a current one for any subcontract flowing from a post-November 2025 prime contract.

Phase 2: The Shift to Mandatory Third-Party Certification

Phase 2 begins on November 10, 2026. At that point, the Department of Defense will begin including mandatory Level 2 C3PAO certification requirements in applicable solicitations and contracts. A self-assessment will no longer satisfy the Level 2 requirement for most contracts involving CUI.

For subcontractors, the effect is direct. If a prime contract awarded after November 10, 2026 requires Level 2 C3PAO certification and the prime needs to flow CUI down to a subcontractor, that subcontractor must hold a current C3PAO-assessed CMMC Level 2 certificate or a conditional CMMC status before the subcontract can be awarded. A self-assessment will not be sufficient.

The conditional certification pathway exists for subcontractors that meet at least 80 percent of the 110 NIST SP 800-171 requirements at the time of their C3PAO assessment. A conditional status is valid for 180 days, during which all remaining deficiencies documented in a Plan of Action and Milestones must be remediated and closed out. If the POA&M items are not resolved within that window, the conditional status expires and the subcontractor is no longer eligible for contracts requiring Level 2 certification.

The assessment capacity constraints make the Phase 2 timeline particularly challenging for subcontractors who have not yet engaged with the process. As of early 2026, approximately 80 authorized C3PAOs serve the entire Defense Industrial Base, assessment wait times are running six months or longer, and organizations that have not begun remediation will not have time to reach readiness before the November deadline. The subcontractors who wait for a formal mandate in their subcontract language before beginning preparation are the ones most likely to miss the window.

What Prime Contractors Are Doing Ahead of the Mandate

The formal CMMC phased rollout is only part of the picture. Many prime contractors have already begun requiring CMMC readiness from their subcontractors as a condition of inclusion in bids and proposals, regardless of whether the specific solicitation formally requires it. This is a risk management decision, not a regulatory one. A prime contractor that includes a non-compliant subcontractor in a proposal risks having that subcontractor become a program liability after award.

In practice, this means that subcontractors are losing competitive position before any formal CMMC clause appears in their subcontract. Supply chain and supplier quality teams at major primes are identifying which subcontractors are CMMC-ready and factoring that into sourcing decisions. Subcontractors that cannot demonstrate progress toward certification are being moved to the bottom of preferred supplier lists or excluded from new bid teams entirely.

For subcontractors who serve as sole-source or limited-source suppliers for critical components, this dynamic creates a different but equally urgent pressure. The prime may not be able to replace them easily, but the prime also cannot afford to have a key supplier unable to receive CUI when the contract requires it. In those cases, the conversation is less about exclusion and more about the prime needing the subcontractor to accelerate their compliance timeline, often with a specific deadline tied to a contract milestone.

False Claims Act Exposure for Subcontractors

The consequences of misrepresenting CMMC compliance extend beyond contract eligibility. The Department of Justice has been actively pursuing cybersecurity-related enforcement under the False Claims Act, and subcontractors are not exempt from that scrutiny. A subcontractor that affirms compliance in SPRS without having actually implemented the required controls is making a

representation to the federal government that can form the basis for a False Claims Act action.

Two recent settlements illustrate the enforcement posture. MORSECORP paid $4.6 million to resolve allegations that it falsely represented compliance with cybersecurity clauses under DoD contracts. Raytheon agreed to pay $8.4 million for allegedly failing to meet required cybersecurity obligations while certifying compliance. In both cases, the enforcement action was triggered by the accuracy of the compliance claim, not by a breach or a cyber incident. The government did not need to demonstrate that data was compromised. It needed to demonstrate that the contractor said it was compliant when it was not.

For subcontractors, this means that posting an SPRS score that is not supported by documented, evidence-based implementation of the underlying controls creates legal exposure that goes well beyond losing a contract. The annual affirmation requirement amplifies this risk, because it requires a named senior official to certify ongoing compliance each year. That affirmation is a statement to the government, and it carries the weight of one.

What Subcontractors Should Be Doing Now

The question of whether a subcontractor can operate without CMMC certification today has a qualified yes, depending on the specific contract and the current phase. The question of whether that subcontractor can continue to operate without certification through the end of 2026 and beyond has a much more definitive answer. The window in which self-assessment alone satisfies Level 2 requirements is closing, and the practical pressures from prime contractors are already narrowing the path for subcontractors that have not started.

Subcontractors handling CUI should be taking several steps now. The first is to complete a legitimate, evidence-based self-assessment against all 110 NIST SP 800-171 controls and post the resulting score to SPRS. This is the minimum requirement for contract eligibility today under Phase 1. The second is to scope the CUI environment accurately, identifying every system that processes, stores, or transmits CUI and ensuring that the boundary between in-scope and out-of-scope

systems is clearly defined and documented. The third is to begin remediation of any control gaps identified in the self-assessment, because those gaps represent the distance between the current state and C3PAO readiness. The fourth is to engage with a C3PAO to understand scheduling availability and begin planning for a formal assessment, recognizing that wait times are already measured in months.

Subcontractors that take these steps now will be positioned to meet Phase 2 requirements when they arrive. Subcontractors that do not will find themselves unable to receive new subcontract awards under contracts that require Level 2 certification, and they will face increasing difficulty maintaining their position in the supply chains of prime contractors who are already evaluating supplier readiness.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced and the founder of a CMMC consulting practice serving Defense Industrial Base contractors and their legal counsel. His work focuses on CMMC readiness, enablement, and implementation services, with particular emphasis on the operational dynamics of compliance across prime and subcontractor relationships. He is an Associate Member of the American Bar Association Section of Public Contract Law and the author of The CMMC Decision. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

32 CFR Part 170, Cybersecurity Maturity Model Certification Program. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170

48 CFR 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements. https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7021

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), Federal Register, September 10, 2025. https://www.federalregister.gov/documents/2025/09/10/2025-17359/

32 CFR 170.23, CMMC Application to Subcontractors.

NIST Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Department of Justice, Civil Cyber-Fraud Initiative, October 2021. https://www.justice.gov/civil/cyber-fraud-initiative

Koran, David W. No Certification, No Contract: What the CMMC Mandate Means for Defense Subcontractor Executives. https://davidkoran.com/white-papers/no-certification-no-contract/

Koran, David W. CMMC Phase 1 Realities: A GAO Gap Analysis. https://davidkoran.com/white-papers/cmmc-phase1-realities-gao-analysis/

Koran, David W. SPRS Score Accuracy and Defensibility. https://davidkoran.com/sprs-score-accuracy/