POLSINELLI

Publications

September 26, 2024 • Updates

CMMC 2.0: Department of Defense Releases New Proposed DFARS Rule to Implement its Cybersecurity Maturity Model Certification 2.0 Program

On August 15, 2024, the U.S. Department of Defense (DoD) published a proposed rule that amends the Defense Federal Acquisition Regulation Supplement (DFARS) to provide the contractual framework for the agency's Cybersecurity Maturity Model Certification (CMMC) 2.0 program. This proposed rule provides guidelines to DoD contracting officers related to incorporating the contractual requirements of the agency's CMMC 2.0 program, including applicability requirements and specific clause language to be included in solicitations and contract awards. The 60-day comment period for this proposed rule is currently open and ends October 15, 2024.

If you are an organization within the DoD supply chain and have not already, you should quickly develop and begin implementing a plan to achieve compliance that makes sense for your organization in light of your potential business opportunities, current cybersecurity posture, and other ongoing security initiatives.

What is CMMC and How Has it Evolved?

As a refresher, the DoD first announced its CMMC program in June 2019 (the early days of CMMC are summarized here). Prior to the CMMC construct, defense contractors were, and currently are today, required to self-certify their compliance with DoD cybersecurity requirements under DFARS 252.204-7012 in a similar manner as many other contractually imposed compliance obligations. CMMC expands on this foundation by imposing more formalized assessment and oversight processes, in many instances involving certification by an independent third party. The ultimate purpose of the CMMC program is to protect sensitive, unclassified information shared or generated between the DoD and its supply chain. It also ensures that defense contractors and subcontractors meet specific cybersecurity requirements, such as the NIST SP 800-171 security controls, that apply to contractor systems processing Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The CMMC program also increases the potential for False Claims Act liability for contractors due to heightened compliance attestation obligations.

Related People

- Erin L. Felix
- Sarah S. Glover
- Mary Ann H. Quinn
- Cate Baskin
- Olivia Velasco

Related Capabilities

- Privacy & Cybersecurity
- Government Contracts

In September 2020, DoD issued an interim final rule implementing a family of new DFARS clauses and provisions. These clauses collectively require DoD contractors and subcontractors to perform prescribed self-assessments against the NIST SP 800-171 standards and file their scores in a centralized government Supplier Performance Risk System (SPRS) database as a condition of award. An additional DFARS clause included with this rule also put contractors on notice of the forthcoming CMMC program and included a contractual 'hook' for its implementation.

In response to significant industry feedback, DoD subsequently announced its revised "CMMC 2.0" program in November 2021. As explained by the agency, CMMC 2.0 has three key features:

- *Tiered Model:* CMMC requires companies entrusted with national security information to implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also describes the process for requiring protection of information flowed down to subcontractors.
- *Assessment Requirement:* CMMC assessments allow the [DoD] to verify the implementation of clear cybersecurity standards.
- *Implementation through Contracts:* Once CMMC is fully implemented, certain DoD contractors handling sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

Where Are We Now?

DoD's formal rollout of its official CMMC program is rapidly approaching as a pair of complementary proposed rules work their way through the federal rulemaking process. Once finalized, the net result of these two rules is expected to be that nearly all recipients of DoD funding—regardless of the company's position in the supply chain—will be required to comply (and formally certify their compliance) with CMMC 2.0 cybersecurity requirements in the vast majority of DoD solicitations and contracts.

First, the government issued a proposed rule in December 2023 delineating the key technical and reporting requirements of the program under what will be a new section of the Code of Federal Regulations at 32 CFR Part 170. The comment period for this proposed rule closed in February 2024, and publication of the final rule is believed to be imminent.

On August 15, 2024, DoD released the second proposed rule relating to CMMC 2.0. This rule will amend the DFARS to require contracting officers to formally incorporate CMMC certification requirements into DoD procurements, making the 32 CFR Part 170 requirements a contractual reality for contractors and subcontractors. Specifically, the proposed rule includes modifying 48 CFR Parts 204, 212, 217, and 252 to:

(1) Add references to the CMMC 2.0 program requirements delineated in the proposed new 32 CFR Part 170;

(2) Add definitions for CUI and DoD-unique identifiers;

(3) Establish a solicitation provision and prescription to be included in all contracts covered by the CMMC 2.0 program; and

(4) Revise the existing DFARS clause language and prescription.

The proposed rule further outlines a three-year phased rollout of the program, commencing with finalization of both the 32 CFR and 48 CFR proposed rules and leading

to full implementation in all covered DoD procurements by Year 4.

Notably, the proposed rule retains and amends contractors' existing compliance obligations under DFARS 252.204-7012. Perhaps most importantly for contractors, they will now be required to report to their contracting officers within ***72 hours*** if they experience "any lapses in information security or changes in the status of the CMMC certificate or CMMC self-assessment levels during performance of the contract." The phrase "lapses in information security" is not defined in the rule, and the ambiguity of this new requirement has the potential to greatly broaden contractors' compliance and reporting burdens. Similarly, the obligation to rapidly report *any* changes to a company's assessment level requires that contractors establish additional mechanisms to proactively and continuously track, identify, and ensure swift reporting of any such potential changes.

When does CMMC apply?

The finalization of both proposed rules will begin a timer on the three-year phase-in period. During this period, if a requirement for CMMC is incorporated into a contract (as determined by the government), the contractor must itself comply and flow down applicable certification requirements to its subcontractors. Once the phase-in period is complete, CMMC will apply to all DoD solicitations and contracts valued above the then-current micro-purchase threshold (defined at FAR 2.101) involving the handling of FCI or CUI; besides the contract value, the only other procurements excluded from CMMC are those for commercially available off-the-shelf items.

When CMMC requirements are incorporated into a contract, contracting officers and higher-tier buyers may not make an award, exercise any options, or extend periods of performance if the contractor has not provided evidence of certification for the required CMMC level based on that solicitation or contract. This evidence of compliance must be established at the time of award and reasserted at least annually in SPRS for all information systems handling FCI or CUI.

Key Takeaways and Next Steps

As noted above, the comment period for the 32 CFR rule is closed, and publication of the final rule is expected imminently. The comment period for the 48 CFR proposed rule is still open, and comments may be submitted until October 15, 2024. Once closed, the government is not required to resolve comments and publish a final rule within a specific timeframe (or ever!). That said, DoD is eager to begin formally implementing its CMMC program as soon as possible, and the agency is expected to prioritize and expedite its internal processing and publish the final rule as soon as possible. While the agency could feasibly still issue the 48 CFR final rule in 2024, early 2025 is likely to be the soonest we would expect to see it officially published.

In the meantime, however, DoD and industry commentators continue to emphasize that contractors and subcontractors should be actively working *now* on their NIST 800-171 implementation and CMMC preparations. DoD contractors have been contractually required to comply with this NIST standard and rapidly report "cyber incidents" since 2016 under the existing DFARS 252.204-7012 clause. While the CMMC 2.0 program makes many of the compliance obligations more stringent and formalized, the foundational requirements are present in DoD contracts and subcontracts today; contracting officers and higher-tier contractors currently may not award contracts unless they have verified that the seller has performed a self-assessment against the NIST 800-171 standards and posted their score in SPRS. Regardless of what happens with these proposed rules, DoD contractors and subcontractors should ensure that their cybersecurity systems are in line with the NIST SP 800-171 security controls to avoid allegations of noncompliance under their current contracts and potential enforcement actions.

Organizations who know they will be within the scope of the CMMC requirements should also begin planning now for security assessment and CMMC certification activities that may be needed for the company to formally evaluate and achieve compliance in a timely manner once the CMMC program is live. Security assessments should be performed at the direction of outside counsel so that the results are protected by the attorney-client privilege.

For questions about DoD's proposed new rule, the CMMC 2.0 program, and how to approach compliance, please contact Sarah Glover at 205.963.7137, Erin Felix at 202.626.8375, or Polsinelli's Government Contracts or Tech Transactions & Data Privacy practice group.