Published on *The National Law Review* https://natlawreview.com

CMMC 2.0: Department of Defense Publishes Final Rule to Establish its Cybersecurity Maturity Model Certification 2.0 Program

Article By:

James W. Kim

Erin L. Felix

After years in the making, on October 15, 2024, the U.S. Department of Defense (DoD) published its final rule to establish the Cybersecurity Maturity Model Certification (CMMC) Program, amending Title 32 of the Code of Federal Regulations ("CMMC Program Rule"). The final rule is **effective December 16, 2024**, and will affect **all prospective and actual DoD contractors and subcontractors**that are handling or will handle DoD information that meets the standards for Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) on a contractor information system during performance of the DoD contract or subcontract.

The proposed version of the final rule was initially published on December 26, 2023, and received over 350 public comments, leaving the DoD with much to consider over the past ten (10) months. Now, this final CMMC rule is in place to ensure that defense contractors, including subcontractors, implement and maintain the required security measures to safeguard FCI and CUI throughout the contract period of performance.

The initial CMMC Program Rule contained a four-phase implementation over a three-year period. This final CMMC Program Rule keeps the phases materially the same, except for extending the period between Phase 1 and Phase 2 by six months—this would allow for a full year between the self-assessment period and formal CMMC certification periods. Hopefully, this helps assuage concerns that have been raised by contractors, giving them some breathing room to ensure compliance.

Aside from this final rule establishing the CMMC Program, the DoD also proposed a rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to address procurement related considerations and requirements related to the CMMC Program Rule ("Acquisition Rule"). This proposed Acquisition Rule is discussed further here and, according to the DoD, is set to be finalized early to mid-2025. Once this DFARS Rule is effective, DoD will begin to include CMMC requirements in solicitations and contracts. Significantly, pursuant to the proposed Acquisition Rule contractors who process, store, or transmit FCI or CUI will need to comply with the appropriate level of CMMC **prior to** contract award.

With these new rules in play, it is imperative—now, more than ever—for organizations to identify and develop a compliance plan to ensure continued success within the DoD supply chain.

CMMC Requirements

As a baseline, this final CMMC Program Rule requires defense contractors to provide adequate security on all covered contractor information systems by implementing the 110 security requirements specified in NIST SP 800-171. Additional requirements include:

- Confirmation that any Cloud Service Providers (CSPs) used by the contractor to handle CUI meet Federal Risk and Authorization Management Program (FedRAMP) Moderate Baseline or the equivalent requirements;
- Flow down of all the requirements to subcontractors who process, store, or transmit CUI; and
- Annual affirmations at every CMMC level.

CMMC provides for varying assessments at three tiered levels detailed in the table below.

Level 1 is meant to address the basic safeguarding of FCI. Notably, DoD requires an annual CMMC Level 1 self-assessment against the 15 safeguarding requirements aligned with FAR clause 52.204-21. Further, there are no explicit documentation requirements for a CMMC Level 1 Self-Assessment.

Level 2 offers broader protection of CUI. For Level 2, an Organization Seeking Assessment (“OSA”) may either self-assess or seek certification from an authorized or accredited CMMC Third Party Assessment Organization (“C3PAO”). Meeting the CMMC Level 2 self-assessment (§ 170.16) or CMMC Level 2 certification assessment (§ 170.17) requirements also satisfies the CMMC Level 1 self-assessment requirements detailed in § 170.15 for the same CMMC Assessment Scope.

At the highest level, CMMC Level 3 security requirements are in place to provide enhanced protections for sensitive DoD CUI. Specifically, for the protection against risk from Advanced Persistent Threats. For Level 3, the DoD has also included a limited set of 24 NIST SP 800-172 Feb 2021 requirements in Table 1 to § 170.14(c)(4). Moreover, a condition to request a Level 3 certification assessment from DCMA DIBCAC is the receipt of a Final Level 2 (C3PAO) CMMC Status. Unfortunately, Level 2 and Level 3 may not be requested nor obtained in a single assessment.

What’s Next?

CMMC’s impact will be significant; the DoD estimates 8350 medium and large entities will be required to meet CMMC Level 2 C3PAO assessment requirements as a condition of contract award. As of now, the DoD may include CMMC requirements on contracts awarded prior to the Acquisition Rule becoming effective, although, doing so will require bilateral contract modification after negotiations.

The increased responsibilities and reporting requirements are also likely to increase contractors’ exposure to liability for any misrepresentations or inaccuracies under the False Claims Act (FCA). There has been a rise in FCA claims relating to cybersecurity in recent months, and the CMMC will add yet another source of potential legal and compliance risk. This necessarily heightens the

importance of internal processes regarding monitoring, auditing, and reporting on these new compliance and certification requirements.

Even though this new CMMC Program Rule will be implemented gradually, organizations should get ahead of the game. The CMMC requirements can be extensive for organizations, and it could take some time—not to mention funding, resources, and outside support—to bring their cybersecurity programs into compliance. The final CMMC Program Rule also makes clear that entities may immediately seek a CMMC certification assessment prior to the Acquisition Rule being finalized and the clause being added to new or existing DoD contracts.

National Law Review, Volume XIV, Number 310