GT GreenbergTraurig

Alert | Government Contracts

October 2024

DoD Publishes Final CMMC Program Rule

Go-To Guide:

- CMMC Program Rule takes effect Dec. 16, 2024, with phased implementation over several years beginning with the finalization of the CMMC contract clauses.
- The program aims to verify contractors' cybersecurity postures and implementation of NIST SP 800-171 requirements through third-party assessments.
- Contractors handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must achieve appropriate CMMC Level certification prior to contract award.
- Subcontractors should communicate with prime contractors to understand specific requirements and timelines for upcoming proposals and quotations.

On Oct. 14, 2024, the Department of Defense (DoD) published the final rule that would implement the Cybersecurity Maturity Model Certification 2.0 (CMMC) Program under 32 CFR Part 170 (Final Rule) to the Federal Register. The Final Rule comes less than 10 months after DoD published the proposed rule, which yielded approximately 361 submissions during the public comment period. The Final Rule takes effect Dec. 16, 2024.

Comments on the proposed rule that would implement the associated contract clause were due Oct. 15, 2024. Once that rule is final, the entire CMMC program will take effect.

The 'Why' for New DIB Contractors

New and prospective Defense Industrial Base (DIB) contractors should understand the rationale for the CMMC Program. As DoD explains in the Final Rule's preamble, the agency has, to date, relied on contractor self-representations and affirmations that they meet the NIST SP 800-171, rev. 2 requirements, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations." However, the DoD has not benefitted from sufficient insight into their contractors' cybersecurity postures and ability to adequately implement the NIST SP 800-171, rev. 2 requirements, particularly throughout the supply chain. Indeed, in 2019, the DoD released findings of its audit that showed critical implementation deficiencies in DoD-mandated system security controls.

The CMMC Program is designed to respond to these gaps by adding third-party verification (through authorized third-party assessment organizations (C3PAOs)) and additional assessment requirements as a condition of contract award. It is important to note that the CMMC Program is, at its core, a verification measure to ensure that contractors are meeting the DFARS 252.204-7012 and 252.204-7020 requirements (in addition to DFARS 252.204-7021, which will be updated pursuant to the 48 CFR rulemaking). CMMC does not impose additional cybersecurity requirements beyond those found in NIST SP 800-171 and SP 800-172. However, once the program is fully implemented, both prime and subcontractors that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must achieve the requisite CMMC Level(s) prior to contract award.

Key Preliminary Takeaways

While much from the proposed rule remains unchanged, the 146-page final rule provides some additional points of clarification.

- Phase 1 Extended. The CMMC Program is still expected to be implemented in four phases, with the first phase beginning when both the Final Rule under this 32 CFR part 170 and the 48 CFR part 204 rule implementing the contract clauses take effect. In response to public comments, DoD has extended Phase 1 by six months under § 170.3(e). Phases 2-4 will each start consecutively one calendar year after the preceding phase. Under the final Phase 4, DoD expects to include the CMMC Program requirements in all applicable solicitations and contracts, including option periods.
- DoD Discretion. DoD retains the discretion to include certain CMMC Level requirements during the phased approach. Pursuant to § 170.3(e), under Phase 1, DoD may include the Level 1 or 2 self-assessment requirements as a condition to exercise an option period on a contract that was awarded prior to the CMMC Program effective date. Further, DoD may also include Level 2 C3PAO requirements for applicable solicitations and contracts even during Phase 1. This reflects DoD's longstanding posture that the CMMC Program is designed to verify implementation of requirements included in DoD contracts since 2017. Indeed, in the Final Rule publication, DoD expressly states that it "expects that the public has utilized the lead-time prior to the publication of this rule to prepare for CMMC implementation."
- Out-of-Scope Assets. The Final Rule defines the asset categories and associated requirements under the scoping provisions of § 170.19. Notably, the Final Rule clarifies that a virtual desktop solution that an external service provider configures to *not* allow any processing, storage, or transmission of FCI (for Level 1) or CUI (for Levels 2 and 3) is considered out-of-scope. While there are no associated documentation requirements under Level 1, for Levels 2 and 3, the contractor must be prepared to justify why the virtual desktop asset in question cannot process, store, or transmit CUI.

- Standards Acceptance—JSVA. The Final Rule affirms that under § 170.20, a contractor that conducted a Joint Surveillance Voluntary Assessment (JSVA) and achieved a perfect 110 score will be certified with Level 2 (C3PAO) status so long as all controls are fully implemented. This means there are no outstanding Plan of Action & Milestones (POA&Ms) describing future plans to fully implement any of the controls at the time of standards acceptance. The validity period will be three years from the date of the original Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) High Assessment. Contractors must conduct the assessment *prior to* the Final Rule's effective date.
- Subcontractor Flowdowns. The Final Rule revises § 170.23 slightly to clarify the obligation to include CMMC requirements in subcontracts. For subcontractors that will only process, store, or transmit FCI (and not CUI), a CMMC Status of Level 1 is required, even if the prime contractor may have a higher CMMC Status requirement. The Final Rule also clarifies that when a prime contract has a CMMC Level 3 requirement, the minimum requirement for a subcontractor processing, storing, or transmitting CUI is a Level 2 C3PAO assessment.
- FedRAMP Equivalency. The Final Rule reiterates the need for cloud service providers (CSPs) that process, store, or transmit CUI to align with the FedRAMP Moderate baseline. In doing so, DoD rejected using the ISO/IEC 27001 certification in favor of the NIST cybersecurity requirements as the appropriate standard. DoD further clarified that where a CSP is only handling Security Protection Data (SPD), or in cases where the external service provider is not a CSP, then FedRAMP certification is not required. Instead, the responsive services shall be assessed as part of the contractor's scope as provided in § 170.19(c)(2)(i).

Takeaways

Contractors should review their DoD contracts to assess where they handle FCI or CUI and make sure they are properly safeguarding the information. In particular, subcontractors should check with their primes to understand what specific requirements and timelines they need to meet to ensure they are included as a team member in upcoming proposals and quotations. Contractors that need a Level 2 C3PAO or higher CMMC status should ensure they go through the proper certification assessment with an authorized or accredited assessor, which may take 6-8 months to schedule. Contractors performing under sensitive DoD programs should also consider communicating with program offices in advance of the formal CMMC rollout to understand whether they may become subject to CMMC Level 3 obligations once Phase 2 begins.

The comment period for the proposed rule under 48 CFR closed on Oct. 15, 2024. Given the relatively small number of public submissions, DoD may adjudicate the comments and issue a final rule quickly. The effective date of the 48 CFR rule may be set for early 2025, which would launch the start of Phase 1 under this 32 CFR part 170 Final Rule.

Authors

This GT Alert was prepared by:

- Eleanor M. Ross | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- Cassidy Kim | +1 415.590.5133 | Cassidy.Kim@gtlaw.com
- Olivia Bellini ˇ | Law Clerk/JD | Northern Virginia

ˇNot admitted to the practice of law.