GT GreenbergTraurig

Alert | Government Contracts

October 2020

DoD's Interim Rule on CMMC: Phased Rollout to Immediately Impact Many Federal Contractors

On Sept. 29, 2020, the Department of Defense (DoD) issued an interim rule, Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), that implements its "Cybersecurity Maturity Model Certification" (CMMC) program.[1] While this implementing regulation has been long-awaited, it also contains an unexpected new cybersecurity assessment requirement that will be **effective this coming Nov. 30**. During the CMMC roll-out period, contractors not subject to the new CMMC requirement nonetheless will be required to self-assess (or have DoD assess) their current cybersecurity compliance and report that status to a DoD website prior to any new DoD contract award or DoD's exercise of any contract option or extension of contract performance.

CMMC builds upon the existing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which establishes cybersecurity standards for federal contractors. CMMC encompasses the basic safeguarding requirements for federal contract information and the security requirements for controlled unclassified information (CUI), and adds a third-party certification requirement that will serve to verify contractors have implemented processes and practices associated with the achievement of one of five cybersecurity maturity levels. The CMMC framework is comprised of five maturity or certification levels, from level 1, "Basic Cyber Hygiene," to level 5,

[1] For more on CMMC, *see* Moorhouse and Przygrodzki, GT Alert, Oct. 7, 2019, "New Cybersecurity Certification Requirements for Government Contractors"; Schipma, Straus and Muenzfeld, Feature Comment, "Cybersecurity For Government Contractors: DOD's New Cybersecurity Model Certification Rapidly Taking Shape," 61 The Government Contractor ¶ 293, Oct. 9, 2019.

"Advanced/Progressive." The interim rule confirms that DoD is implementing a phased rollout of CMMC assessment requirements from Nov. 30, 2020 (the effective date for the interim rule) through Sept. 30, 2025. The interim rule also adds and amends DFARS subparts and clauses to implement CMMC.

This interim rule first adds a new DFARS Subpart 204.75, Cybersecurity Maturity Model Certification (CMMC). This subpart lays out the policies and procedures for awarding a contract or exercising an option on a contract between Nov. 30, 2020, and Oct. 1, 2025. This subpart requires contractors to achieve at the time of award a CMMC certificate at the level specified in the solicitation. Contractors must maintain a current (i.e., not more than three years old) CMMC certificate at the specified level throughout the life of the contract or task or delivery order. Contracting officers are prohibited from exercising an option period or extending the period of performance on the contract, task or delivery order to a contractor that does not have a current CMMC certification at the required level. CMMC certification will be identified in the Supplier Performance Risk System (SPRS), and contracting officers are required to verify an offeror or contractor's CMMC level in the system.

The interim rule also establishes and prescribes DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement, which eventually will be used in all solicitations and contracts, task, or delivery orders (excluding acquisitions exclusively for commercial off-the-shelf (COTS) items). During phase-in of CMMC requirements, this clause only will be incorporated in DoD contracts that need immediate CMMC Certification (i.e., third-party assessment conducted and the issuance of a CMMC Certification). The Under Secretary of Defense for Acquisition and Sustainment (USD A&S) will determine which solicitations will be subject to the CMMC requirement, and such covered contracts will include the DFARS 252.204-7021. Procurements subject to the CMMC requirement will include the new DFARS clause, and the statement of work will require a contractor to have met the requirements of a specified CMMC level. Beginning Oct. 1, 2025, it will appear in all solicitations, contracts, task or delivery orders (excluding acquisitions for COTS items) that are above the micro-purchase threshold. The clause requires a contractor to:

- have a current (i.e., not older than three years) CMMC certificate at the CMMC level required by the contract;
- maintain the CMMC at the required level for the duration of the contract;
- flow down the substance of the clause in all subcontracts and other contractual agreements (excluding COTS items); and
- ensure that a subcontractor has a current CMMC certificate at the CMMC level appropriate for the information that is being flowed down to the subcontractor before making award to the subcontractor.

The interim rule also promulgates a new DFARS provision and clause that address contractor assessment requirements. The interim rule directs contracting officers to include a new DFARS provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, and a new DFARS clause 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, in solicitations and contracts including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.

The new DFARS provision 252.204-7019 advises offerors of the new assessment requirement, while the new DFARS clause 252.204-7020, DoD Assessment Requirements, requires DoD contractors to immediately post Assessments of their cybersecurity compliance on the DoD's SPRS. Prime contractors are required to flow down the substance of DFARS 252.204-7020 to all subcontractors (excluding COTS suppliers). Prior to awarding a subcontract (or other contractual instrument) subject to the

implementation of NIST SP 800-171 requirements, prime contractors must also ensure that the subcontractors have a current DoD Assessment posted in SPRS that was completed in the last three years. If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment posted in SPRS, the rule explains that the subcontractor is permitted to conduct and submit a Basic Assessment to DoD for posting to SPRS along with the information required by paragraph (d) of the clause. Subcontractors at all tiers should be aware of this requirement and ensure compliance with the same to maintain eligibility for awards.

While the full implications and potential issues associated with the phased rollout of CMMC are not yet clear, the interim rule clarifies that the impact for many federal contractors will be immediate. As a result, federal contractors should assess their existing and impending obligations under CMMC, and take all necessary actions to ensure compliance.

Authors

This GT Alert was prepared by:

- Scott A. Schipma | +1 202.331.3141 | schipmas@gtlaw.com
- Danielle K. Muenzfeld | +1 202.533.2393 | muenzfeldd@gtlaw.com