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

DoD Advances CMMC: Key Takeaways from the Proposed August 2024 DFARS Rule

Article By:

Ben Squires

On August 15, 2024, the US Department of Defense (DoD) published a proposed rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) in order to implement the Cybersecurity Maturity Model Certification (CMMC) program. DoD is executing a phased rollout of CMMC, and the August 2024 proposed rule is the second proposed rule DoD has published as part of its implementation.

Background

DoD issued a proposed CMMC rule on December 26, 2023. Specifically, the December 2023 proposed rule would formally establish the CMMC program by adding a new Part 170 to Title 32 of the Code of Federal Regulations. The December 2023 proposed rule would codify requirements for three CMMC levels:

Level 1 for basic safeguarding of Federal contract information (FCI) for contractors that handle FCI but not controlled unclassified information (CUI)

Level 2 for the broad protection of CUI for contractors and subcontractors that handle CUI

Level 3 for higher-level protection of CUI against risk from Advanced Persistent Threats (APTs), with applicability to be determined by DoD for each contract based on the sensitivity of the CUI involved

The rule details the security controls applicable to each of the three CMMC levels and the process for the assessment, as well as certification of these levels for contractors to prove compliance. The December 2023 proposed rule is still pending as of September 3, 2024.

As discussed in detail below, the August 2024 proposed rule will apply CMMC through a new DFARS rule by making additions and revisions to the DFARS to detail the standard clauses that contracting officers must include in all DoD solicitations and contracts covered by CMMC.

Details of the August 2024 Proposed Rule

The August 2024 proposed rule prescribes a new clause at DFARS 252.204-7YYY that contracting

officers must insert in solicitations to identify the CMMC level applicable to the contract. The August 2024 proposed rule also revises the clause at DFARS 252.204-7021 to incorporate the requirements of CMMC into contracts that involve the handling of FCI or CUI. These requirements would apply to all DoD solicitations and contracts, including those for the acquisition of commercial products or commercial services. However, this clause would not apply to acquisitions for commercially available off-the-shelf (COTS) items or contracts below the micro-purchase threshold, currently US$10,000 for most procurements.

Particularly, the August 2024 proposed rule would require contractors that handle FCI and CUI have the results of a current CMMC certificate or CMMC self-assessment, at the level required, at the time of award. The August 2024 proposed rule underscores that the CMMC level specified in a solicitation or contract "is required for all information systems, used in the performance of the contract, that will process, store or transmit" FCI or CUI, as applicable. The requisite CMMC level must be maintained for the entire life of the contract for all applicable information systems.

Notably, the August 2024 proposed rule would require contractors to notify their contracting officers within 72 hours anytime they experience "any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract." This appears to be a broader requirement than the current DFARS 252.204-7012 requirement for contractors to report "cyber incidents" within 72 hours. The term "cyber incident" is defined at DFARS 252.204-7012(a) as "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." Unfortunately, the August 2024 proposed rule does not define lapses in information security and does not limit the reporting requirement to only those affecting covered information systems or the CUI or FCI residing on those systems, as it does in DFARS 252.204-7012. Hopefully, the final rule will provide a definition of this term. The August 2024 proposed rule also requires that contractors notify each individual contracting officer when a lapse occurs, rather than via DIBNet, as is required in DFARS 252.204-7012. This would be a significant burden to contractors especially those that have numerous contracts.

The August 2024 proposed rule includes a standard solicitation provision DFARS 252.204-7YYY for inclusion in all solicitations for contracts covered by the CMMC program. This provision would require contracting officers to provide notice to offerors of the CMMC level required by the solicitation, and of the CMMC certificate or self-assessment results that are required. Successful offerors would also be required to provide the DoD unique identifier issued by the Supplier Performance Risk System (SPRS) for the contractor information systems that will process, store or transmit FCI or CUI during contract performance at the contracting officer's request. Contractors and subcontractors will also need to complete and maintain an affirmation of continuous compliance in the SPRS annually, or when a change to CMMC compliance status occurs, for the relevant security requirements depending on the CMMC level.

Note that the August 2024 proposed rule requires CMMC Level 1 contracts to maintain a self-assessment that is not older than one year, so long as there have been no changes in CMMC compliance since the assessment. CMMC Levels 2 and 3 require a certificate (or self-assessment if applicable to Level 2) that is not older than three years, so long as there have been no changes in CMMC compliance since the certification or assessment. The offeror must have a current affirmation of continuous compliance with the security requirements identified in SPRS prior to award. Affirmations must not be older than one year if there have been no changes in CMMC compliance since the affirmation. Finally, contracting officers may not exercise options on contracts and orders without a current CMMC certificate or self-assessment and affirmation of continuous compliance for

each information system that processes, stores or transmit FCI and CUI.

The proposed revisions to DFARS 252.204-7021 must be flowed down to subcontractors at all tiers, when the subcontractor will process, store, or transmit FCI or CUI, based on the sensitivity of the unclassified information flowed down to each.

Comments on the August 2024 proposed rule are due on or before October 15, 2024.

National Law Review, Volume XIV, Number 254