Westlaw Today
powered by Reuters

DoD's proposed rule would implement CMMC contract clauses

By Eleanor M. Ross, Esq., Cassidy Kim, Esq., and Jeffery M. Chiow, Esq., Greenberg Traurig LLP*

AUGUST 28, 2024

Go-to guide:

- **A requirement to bid or perform.** If the Department of Defense (DoD)'s Proposed Rule is finalized, defense contractors would be required to meet all security requirements of the specified Cybersecurity Maturity Model Certification (CMMC) level at the time of contract award and throughout the life of the contract for all information systems that will process, store, or transmit federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.
- **Every DoD contract over $10K, except COTS.** The new clauses would apply in solicitations and contracts, task orders, or delivery orders that require the contractor to have a specific CMMC level, including solicitations and contracts for commercial products and services (except for commercial-off-the-shelf items) over the micropurchase threshold.
- **Must specify the relevant information system(s).** Offerors and contractors would be required to identify the contractor information systems that would be used to process, store, or transmit FCI or CUI in performance of the contract prior to award, exercise of an option, or extension of any period of performance.
- **Annual certification by senior company official.** Contractors would also be required to complete an annual affirmation of continuous compliance with the applicable security requirements. A senior company official would be required to complete the affirmation.
- **Effective beginning in FY25.** Comments on the proposed regulations are due Oct. 15, 2024. The rule could be finalized as soon as Spring 2025.

On Aug. 15, 2024, DoD published (https://bit.ly/3MknIVk) a proposed rule to implement contract clauses related to the proposed CMMC Program (Proposed Rule). DoD previously published a related proposed rule (https://bit.ly/4dVP7IV) implementing the CMMC 2.0 Program in 32 CFR 170.

The earlier proposed rule provided the details of the CMMC Program implementation and the security requirements. This latest Proposed Rule introduces the contractual clauses to implement the CMMC Program and modifies the original CMMC contract clause drafted in a Sept. 29, 2020, interim rule implementing the original CMMC Program (DFARS 252.204-7021).

The Proposed Rule would make changes to Title 48 of the Code of Federal Regulations and add new contract clauses to implement the CMMC Program in DoD contracts. The Proposed Rule revises the Defense Federal Acquisition Regulation Supplement (DFARS) to include contract clauses to implement the CMMC Program described in 32 CFR Part 170.

The new clauses would apply in solicitations and contracts, task orders, or delivery orders that require the contractor to have a specific CMMC level.

The Proposed Rule adds two new contract clauses: DFARS 252.204-7XXX, Notice of Cybersecurity Maturity Model Certification Level Requirements and DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements. Both clauses serve to identify the CMMC level applicable to any solicitation or contract.

Key elements of the contract clauses

Under the Proposed Rule, contractors would be required to have the results of their CMMC certificate or self-assessment entered into SPRS at the CMMC level specified in the above contract clauses at the time of contract award.

Contractors would also need to have an affirmation of continuous compliance with the security requirements identified in 32 CFR 170 in the Supplier Performance Risk System (SPRS) for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in the performance of the contract.

For each contractor information system that processes, stores, or transmits CUI, the contractor would post the self-assessment or certification in SPRS, which would generate a DoD unique identifier (DoD UID) for the assessment and information system. That DoD UID would be reported to the contracting officer for each contractor

information system that processes, stores, or transmits FCI or CUI during the performance of the contract.

In addition:

- The contractor would be required to have and maintain the requisite CMMC level for the life of the contract.
- The contractor would need to complete and maintain on an annual basis, or when security changes occur, the affirmation of continuous compliance with the security requirements in 32 CFR 170. The affirmation would need to be made by a senior company official for each DoD UID applicable to the contractor information systems that process, store, or transmit FCI or CUI during contract performance. The affirmation would attest that the self-assessment or certification remains current and that the system complies with the security requirements in 32 CFR 170.
- The contractor would need to notify the contracting officer of any changes in the contractor information systems that process, store, or transmit FCI or CUI during contract performance, including any updates to the corresponding DoD UIDs.
- The contractor would need to ensure that its subcontractors have the appropriate CMMC level prior to awarding a subcontract or other contractual instrument. The requirements of the clause must be included in subcontracts or other contractual instruments at all tiers so long as the subcontractor is processing, storing, or transmitting FCI or CUI.

The contractor would need to ensure that its subcontractors have the appropriate CMMC level prior to awarding a subcontract or other contractual instrument.

In addition to these requirements, the Proposed Rule also proposes amendments to Part 212 (to incorporate the new clauses into solicitations and contracts for commercial items), Subpart 217.207 (to ensure that options are exercised in accordance with the new clauses), and Subpart 204.75 (to add definitions, policy, procedures, and the application of the contract clauses).

Implementation

The Proposed Rule contemplates the same phased approach to implementation outlined in the previous CMMC Program rulemaking.

For the first three years after the final rule's effective date, the requirements would only impact an offeror or contractor when the solicitation or contract requires an offeror or contractor to have a specific CMMC level. By the fourth year, all covered solicitations and contracts, task orders, and delivery orders would have a required CMMC level.

In the Proposed Rule, DoD assessed the impact of complying with the contract clause requirements: posting the results of a CMMC self-assessment to SPRS, completing the required affirmation, and retrieving DoD UID information for the information systems that would be used in the performance of a specific contract or solicitation.

DoD also estimates that in year one, approximately 1,104 small entities would be subject to the new rule, and by the fourth year, approximately 20,395 small entities would be impacted.

For each of these tasks, the government estimated that contractors would need to spend five minutes to complete the action. This includes the time for reviewing instructions, gathering and maintaining the data needed, and completing and reviewing the collection of information.

DoD also estimates that in year one, approximately 1,104 small entities would be subject to the new rule, and by the fourth year, approximately 20,395 small entities would be impacted based on the current number of unique entities with DFARS 252.204-7012 contracts.

This figure represents nearly 70% of the total entities that are expected to be impacted and reflects DoD's consistently held position that small businesses are not entitled to categorical cost relief under the new rule.

Next steps

Comments on the Proposed Rule are due Oct. 15, 2024. Interested contractors should plan to submit comments on areas of concern or places where further clarification is required. Given the impact of the new rule, DoD will likely receive extensive comments from interested parties.

Once the comments have been received and reviewed, the government must respond to each comment, explaining why it has or has not made a corresponding change in the Proposed Rule. This may be done in conjunction with the previously released proposed rule implementing the CMMC Program at 32 CFR 170. Once both rules have been finalized, phased implementation of the CMMC Program is scheduled to begin on the effective date of the new rules.

About the authors



Eleanor M. Ross (L), a government contracts associate in the Washington, D.C., office of **Greenberg Traurig LLP**, advises clients on contract disputes, investigations, compliance with federal and state programs, and bid protests. She can be reached at eleanor.ross@gtlaw.com. **Cassidy Kim** (C), a government contracts associate in the firm's San Francisco office, focuses on cybersecurity, privacy and regulatory compliance issues, contract disputes and claims, and bid protests. She can be reached at cassidy.kim@gtlaw.com.

Jeffery M. Chiow (R) is a shareholder, co-chair of the firm's government contracts practice and leader of its defense, aviation and space industry initiative. He represents clients in litigation, bid protests, and investigations and deals involving public contracts. He is based in Washington, D.C., and can be reached at jeff.chiow@gtlaw.com. This article was originally published Aug. 15, 2024, on the firm's website. Republished with permission.

This article was published on Westlaw Today on August 28, 2024.