WINSTON & STRAWN LLP

BLOG

The DOD Proposes DFARS Amendments to Promote Contractor Compliance with CMMC 2.0

SEPTEMBER 30, 2024

Last month, the U.S. Department of Defense (DOD) published a Proposed Rule setting out planned revisions to the Defense Federal Acquisition Regulations (DFARS) to implement the requirements of the Cybersecurity Maturity Model Certification program (CMMC 2.0) proposed in December 2023.[1] CMMC 2.0 is a framework for verifying a DOD contractor's implementation of cybersecurity measures that the DOD requires to protect sensitive unclassified information including Controlled Unclassified Information (CUI), and Federal Contract Information (FCI). The Proposed Rule revises the DFARS to reference the CMMC 2.0 requirements that were proposed in December 2023. This includes changes to the existing CMMC clause at DFARS 252.204-7021, the creation of a new solicitation provision to accompany DFARS 252.204-7021 which will provide notice of the CMMC 2.0 requirement, the establishment of a plan for a phased rollout of the Proposed Rule, and the addition of certain new definitions. The Proposed Rule's comment period ends on October 15, 2024.

CHANGES TO DFARS 252.204.7021

The changes to DFARS 252.204-7021 envisioned by the Proposed Rule include the following:

- Requires contractors to have the CMMC certification or self-assessment [2] at the level required by the contracting officer for all systems used in performance of the contract that process, store, or transmit FCI or CUI, and to maintain this CMMC level for the life of the contract. *See* DFARS 252.204-7021(b)(2) at 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024).
- Requires contractors to complete and maintain an affirmation of continuous compliance with the required CMMC level in the Supplier Performance Risk System (SPRS) for the aforementioned systems, and have a senior company official affirm continuous compliance with security requirements under a contract subject to CMMC requirements on an annual basis. *See* DFARS 252.204-7021(b)(5) at 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024); *see also* 32 C.F.R. part 170, 88 Fed. Reg. 89058, 89136 (Dec. 26, 2023).
- Requires contractors to "notify the Contracting Officer within 72 hours when there are any lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract." *See* DFARS 252.204-7021(b)(4) at 89 Fed. Reg. 66327,66338 (Aug. 15, 2024).
- Requires contractors to include CMMC requirements in any subcontracts and ensure that all subcontractors and suppliers comply with the new CMMC requirements. *See* DFARS 252.204-7021(b)(6) and DFARS 252.204-7021(d) at

89 Fed. Reg. 66327, 66338 (Aug. 15, 2024).

ADDITION OF DFARS 252.204.7YYY

The Proposed Rule would also add a new DFARS clause titled "Notice of Cybersecurity Maturity Model Certification Level Requirements." *See* DFARS 252.204-7YYY at 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024). The DOD proposes to require this clause in solicitations that include DFARS 252.204-7021 and would require the issuing agency to (1) include language identifying the specific CMMC level required for the contract and (2) notify offerors that the apparently successful offeror will not be eligible for award of a contract, task order, or delivery order under the solicitation if the offeror has not posted the results of their CMMC assessment to SPRS at the required level. *See* DFARS 252.204-7YYY(b)(1) and (b)(2) at 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024). This new clause also would require contractors to submit to the contracting officer the unique identifier issued by SPRS for systems used in performance of the contract that process, store, or transmit FCI or CUI. *See* DFARS 252.204-7YYY(c) at 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024).

ROLLOUT AND DEFINITIONS

The Proposed Rule would make other changes, such as adding a definition for CUI, which cites and is substantially similar to the existing definition of CUI in 32 C.F.R. part 2002.4(h). It also proposes a new definition for DOD unique identifier, which is necessary given the new requirements of the Proposed Rule. The Proposed Rule also establishes the DOD's plan to roll out the CMMC requirement over three years once the Proposed Rule is finalized. Under this proposed rollout plan, in the first three years, the CMMC requirement will only be included in certain contracts, but thereafter, the CMMC requirement will be mandatory in all DOD solicitations involving the processing, storage, and transmittal of FCI and CUI.

CONCLUSION

While the DOD's proposed changes in the new rule are neither revolutionary nor unexpected, they remind federal contractors of the DOD's growing insistence that contractors must ensure they meet the DOD's increased cybersecurity compliance requirements. Contractors who fail to meet these cybersecurity requirements will expose themselves to substantial risk from lawsuits and other penalties.[3] Once the DOD implements the Final Rule, however, it will be impossible for contractors to do business with the DOD without clear proof of their compliance with the DOD's latest cybersecurity requirements. Consequently, defense contractors should prepare themselves now to do what is necessary in order to ensure that they are, or soon will be, compliant with the DOD's new cybersecurity requirements.

OUR RELEVANT CAPABILITIES

Winston & Strawn LLP's Government Contracts & Grants Practice comprises a nationally recognized, highly regarded group of lawyers with deep experience in handling high-value, and often contentious, government contract disputes, bid protests, and claims across a broad spectrum of industries and issues. We have a wealth of experience in counseling on the FAR, Grant Regulations, and related supplements, including, but not limited to, rules for cybersecurity compliance. We help contractors navigate these requirements to ensure compliance and address potential issues before expensive investigations, litigation, and attendant reputational damage arise.

Please contact Winston's Government Contracts & Grants team if you have questions about the Proposed Rule or its implications for your business.

---

[1] The Proposed Rule also "partially implements section 1648 of the National Defense Authorization Act for Fiscal Year 2020 (Pub. L. 116-92), which directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the US DIB no later than Feb 1, 2020." 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024).

[2] The Proposed Rule amends DFARS 204-7502 to require contractors to "achieve, at time of award, a CMMC certificate or CMMC self-assessment at the level specified in the solicitation, or higher." 89 Fed. Reg. 66327, 66337 (Aug. 15, 2024); *see also* DFARS 252.204-7YYY(b)(2) at 89 Fed. Reg. 66327, 66338 (Aug. 15, 2024).

[3] *See, e.g.*, DOJ Press Release on August 22, 2024 “United States Files Suit Against the Georgia Institute of Technology and Georgia Tech Research Corporation Alleging Cybersecurity Violations,” available at https://www.justice.gov/opa/pr/united-states-files-suit-against-georgia-institute-technology-and-georgia-tech-research.

5 Min Read

Authors

William T. Kirkwood

Lawrence S. Sher

Lawrence “Larry” Block

Elizabeth Leavy

Frank V. DiNicola

Michael Hill

Related Topics

United States Department of Defense

Defense Federal Acquisition Regulation Supplement

Government Contracts

Cybersecurity Maturity Model Certification Program

Cybersecurity Compliance

Related Capabilities

Government Contracts & Grants

Related Professionals

William T. Kirkwood

Lawrence S. Sher

Lawrence “Larry” Block

Elizabeth Leavy

Frank V. DiNicola

Michael Hill

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.