JENNER & BLOCK

Department of Defense Marches Forward with CMMC Requirements in Proposed Rule

Client Alerts

September 6, 2024
By: Moshe B. Broder, Matthew L. Haws

On August 15, 2024, the Department of Defense (DoD) issued a proposed rule to incorporate contractual requirements related to the proposed Cybersecurity Maturity Model Certification (CMMC) 2.0 program.

While implementation details remain outstanding, DoD's proposed rule sends a strong message to contractors that compliance with CMMC is a matter of when, not if.

This proposed rule includes a new Defense Federal Acquisition Regulation Supplement (DFARS) provision, 252.204-7YYY, Notice of Cybersecurity Maturity Model Certification Level Requirements, 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 to have been posted in the Supplier Performance Risk System (SPRS) by the apparently successful offeror prior to award.

As background, DoD's overarching objective is to ensure that defense industrial base contractors can adequately protect sensitive unclassified information at a level commensurate with the risk, including information shared with subcontractors.

To recap our discussion in previous updates, CMMC Level 1 requires implementing the 15 basic safeguarding requirements set forth in FAR 52.204-21. CMMC Level 2 additionally requires implementing the more expansive 110 security controls identified in NIST SP 800-171 Rev. 2, also required under DFARS 252.204-7012. CMMC Level 3 further requires implementation of the 24 select requirements in NIST SP 800-172, intended to counter the risk from advanced persistent threats.

Consistent with DoD's proposed rule issued on December 26, 2023 (88 FR 89058), this second proposed rule continues to contemplate self-assessment for CMMC Level 1, the possibility of either self-assessment or third-party assessment for CMMC Level 2, and DoD assessments for CMMC Level 3. The levels and assessments will be reported to SPRS.

The proposed rule explains that the contracting officer will specify in a solicitation provision which CMMC level is required, and the contracting officer shall not award a contract to an offeror that lacks

the requisite CMMC certification or self-assessment at the specified level. The contracting officer must also verify that the contractor has a "current affirmation of continuous compliance" with the CMMC requirements submitted in SPRS for each contractor information system that will process, store, or transmit federal contract information (FCI) or controlled unclassified information (CUI) in performance of the contract. The same requirements apply with respect to exercising an option period or extending the period of performance on a contract, where the contract includes the CMMC clause.

Importantly, the proposed rule anticipates a gradual phase-in over a three-year period. DoD explains that during the first three years of the phased rollout, the CMMC Program Office will direct DoD component program offices to include CMMC requirements in certain contracts. After three years, however, all DoD component program offices must include CMMC requirements in solicitations and contracts where the contractor will process FCI or CUI on contractor information systems.

The proposed rule introduces new ambiguities likely to draw comments from industry. Notably, the proposed revisions to DFARS 252.204-7021 mandate that contractors notify the contracting officer within 72 hours of any "lapses in information security or changes in the status of CMMC certificate or CMMC self-assessment levels during performance of the contract." The 72-hour requirement is presumably intended to mirror the current "cyber incident" reporting requirement in DFARS 252.204-7012,[1] however the scope of this notification requirement is unclear and arguably very broad. What constitutes a "lapse" or a "change in status"? The volume of notifications to contracting officers could create unintended administrative burdens, not to mention divergent interpretations of these undefined terms. Furthermore, the risk of enforcement or False Claims Act (FCA) liability remains in the background as the Department of Justice has allocated resources to its Civil Cyber-Fraud Task Force and pursued non-compliance with contractual cyber requirements as a basis for FCA liability.

More broadly, the proposed requirement to notify contracting officers of a "lapse" or change in CMMC status reflects how far the regulations have progressed from the self-certification regime of DFARS 252.204-7012, to reporting on the extent of compliance through self-assessments and government assessments under DFARS 252.204-7019 and -7020, and now to third-party assessments with notification to contracting officers in the event of lapses or changes.

Another important consideration for contractors is whether and where CUI resides on a contractor information system. This is a threshold determination from which compliance obligations flow. As the proposed rule confirms, "if there is a requirement for CMMC, then it applies to all information systems that process, store, or transmit FCI or CUI in performance of the contract." Conversely, if a contractor (or subcontractor) information system does not process, store, or transmit FCI or CUI in performance of the contract, it need not receive a CMMC assessment or certification. The flow of information and system boundaries thus becomes an important practical implementation consideration.

Finally, under the proposed revision to DFARS 252.204-7012, prime contractors are required to ensure that subcontractors “and suppliers” annually affirm continuous compliance with the security requirements associated with the CMMC level required for the subcontract or other contractual instrument for each of the contractor information systems that process, store, or transmit FCI or CUI and that are used in performance of the contract. While commentors requested that DoD roll out a tool for prime contractors to validate subcontract CMMC certificates and self-assessments, DoD acknowledged that there is currently no such tool, and prime contractors are instead “expected to work with their suppliers to conduct verifications as they would under any other clause requirement that applies to subcontractors."

Comments regarding this proposed rule are due no later than October 15, 2024. As with prior rulemakings related to CMMC, a significant number of comments are expected to be submitted. Given the time necessary to adjudicate comments and issue a final rule, the beginning of the gradual phased rollout is not expected to begin until some point in 2025.

Footnotes

[1] There is no parallel notification requirement under FAR 52.204-21, so implementation of this clause will create new notification requirements for contractors reporting lapses in compliance with these security controls.

Related Attorneys

Moshe B. Broder
Partner
mbroder@jenner.com
+1 202 637 6334

Matthew L. Haws
Partner
mhaws@jenner.com
+1 202 639 6065

Related Capabilities

Government Contractor Litigation and Compliance

Stay Informed →