wiley

ALERT

CMMC 2.0 Update: DOD Proposed Rule Introduces Standard Terms for Contracts Subject to CMMC 2.0, Including Yet Another 72-Hour Notification Requirement

August 15, 2024

WHAT: The U.S. Department of Defense (DOD) just published the second of two proposed rules setting forth key requirements for its long-anticipated Cybersecurity Maturity Model Certification (CMMC) 2.0 program. The earlier proposed rule (published in December 2023, and summarized here) outlined the substantive security requirements. This latest proposed rule provides additional guidance to contracting officers, including standard clauses that contracting officers must include in all solicitations and contracts covered by the CMMC 2.0 program.

WHEN: DOD published the proposed rule on August 15, 2024, with a 60-day comment period (through Monday, October 14, 2024). The proposed rule also reaffirms DOD's commitment to a three-year phase-in period, as DOD previewed in the earlier proposed rule.

WHAT DOES THIS MEAN FOR INDUSTRY: For those already following DOD's CMMC 2.0 program, this new proposed rule is significant for two reasons. First, it brings the CMMC 2.0 program one step closer to reality. DOD had previously committed that it would begin phasing in these requirements only after it amended both Title 32 of the Code of Federal Regulations (where the substantive security requirements reside) and Title 48 (where the Defense Federal Acquisition Regulation Supplement resides). Now that DOD has issued proposed rules to amend both, all that remains is for DOD to adjudicate any comments that it receives and publish final rules. Second, this new proposed rule includes a few additional concepts not previously

Authors

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Practice Areas

Cybersecurity
Government Contracts
National Security
Privacy, Cyber & Data Governance

covered by DOD's earlier proposed rule. Most significant, the new proposed rule would require contractors to notify the individual contracting officers within 72 hours of "any lapses in information security."

Many Elements of the CMMC 2.0 Program Remain Unchanged

As a reminder of the CMMC 2.0 rulemaking history, the December 2023 proposed rule provided guidance on security, assessment, and affirmation requirements for DOD prime and subcontractors that handle federal contract information (FCI) and controlled unclassified information (CUI). Most notably, contractors would be required to include affirmations and either self-assessments or third-party certifications attesting to their compliance with varying cybersecurity requirements. This could include the basic security controls for handling FCI (set forth in FAR 52.204-2), the NIST SP 800-171 Rev. 2 security controls (set forth in DFARS 252.204-7012), and potentially the additional controls from NIST SP 800-172 (for CMMC Level 3). The specific security requirements would depend on which CMMC "level" DOD program managers and requiring activities assign to the contract based on the type of information (FCI or CUI) that the contractor would handle on its information system. DOD anticipated that roughly 63% of DOD contracting entities would have to meet "Level 1," the lowest level, whereas 36% would have to meet "Level 2," and 1% would have to meet "Level 3," the highest level.

DOD's August 15 proposed rule provides the contracting mechanisms to implement the 2023 proposed rule by addressing the standard clauses that contracting officers must include in all solicitations and contracts covered by the CMMC 2.0 program. Consistent with DOD's plans in the earlier proposed rule, this new proposed rule would apply to all DOD acquisitions with narrow exceptions exclusively to commercially available off-the-shelf (COTS) items and contracts below the micro-purchase threshold (currently $10,000 for most procurements). DOD estimated that about 29,543 entities would be impacted by contractual requirements for implementing DOD's CMMC framework, 69% of which are small businesses. This number may grow, however, if DOD borrows the standard clauses for the CMMC 2.0 program for other transaction agreements, grants, and other non-procurement contracts, which are beyond the reach of the DFARS – and thus this proposed rule. DOD's estimates also do not include subcontractors, which are subject to CMMC through flowdowns from covered prime contracts. DOD also reiterated its estimated percentage breakdown of entities that will be subject to Levels 1, 2, and 3.

In Articulating the Contract Terms, DOD Has Introduced Some Key Changes and Ambiguities

The August 15 proposed rule supplements DOD's December 2023 proposed rule by providing three components: (1) guidance to contracting officers, (2) a standard contract clause to be included in all contracts covered by the CMMC 2.0 program (DFARS 252.204-7021), and (3) a standard solicitation provision to be included in all solicitations for contracts covered by the CMMC 2.0 program (DFARS 252.204-7YYY). These components largely incorporate the framework laid out by the December 2023 proposed rule in Title 32 of the Code of Federal Regulations, but they add a few new significant – and potentially challenging – concepts worth highlighting.

Report All "Lapses," Rapidly, to All Contracting Officers: The proposed contract clause introduces one of the most puzzling incident reporting requirements yet. The proposed clause would require contractors to notify their contracting officers within 72 hours anytime they experience "any lapses in information security." Proposed DFARS 252.204-7021(b)(4). This would significantly alter the incident reporting regime established in the existing DFARS 252.204-7012 in at least three ways.

- First, DOD selected an amorphous trigger: "any lapses in information security." Each undefined term in this phrase has the potential to be interpreted much more broadly than "cyber incidents," which DOD at least attempted to define in the existing -7012 clause.
- Second, unlike in the -7012 clause, DOD has not clearly limited reportable "lapses" to only those affecting covered information systems or the CUI or FCI residing on those systems.
- Third, DOD proposes to decentralize the reporting regime so that contractors would have to notify each individual contracting officer of any such "lapses." This again differs from the -7012 clause requirement to report "cyber incidents" through DOD's central repository, the DIBNet.

This proposal is likely to frustrate industry, particularly at a time when reporting obligations are proliferating and the U.S. Department of Justice has suggested that a failure to report may be a false claim, as opposed to an administrative or contractual issue. The government has not been shy about bringing such claims, has publicly touted settlements, and has intervened in high profile litigation.

Beware of "Changes in CMMC Compliance." The proposed contract clause previews that some degree of change that a contractor makes to its information system could invalidate an existing certification or self-assessment. The proposed clause does so by defining a "current" CMMC certification as one "with no changes in CMMC compliance since the date of the assessment." Proposed DFARS 252.204-7021. But neither this latest nor the December 2023 proposed rule clarifies what type of "changes" might exceed this threshold.

Only Use CMMC-Certified Information Systems for "Data." The proposed contract clause would require contractors to use only information systems that have an appropriate CMMC certification. Proposed DFARS 252.204-7021(b)(3). Although this might sound intuitive at first, DOD's proposed clause lacks much-needed nuance. For example, the clause is not limited to specific types of information covered by the CMMC 2.0 program (e.g., FCI, CUI) or information that is not yet encrypted for external transmission (as NIST 800-171, Rev. 2, Requirement 3.13.8 contemplates); it simply applies to processing, storing, or transmitting "data." It also makes no distinction for what types of information systems are capable of being certified under the CMMC program. CMMC 2.0 is limited to contractor information systems, thus leaving open questions about whether contractors can now "process, store, or transmit data" on information systems owned or operated by entities that are not subject to CMMC, including government agencies. We anticipate that this overly inclusive language will be a significant topic for stakeholder comment.

A High-Watermark Approach Despite Multiple Enclaves? The proposed solicitation provision is designed to allow contracting officers to identify the CMMC certification or self-assessment level required for the contract. But it, too, lacks nuance. For example, the proposed provision contemplates that the single certification or self-

assessment level identified by the contracting officer will apply "for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during the performance of the contract." Proposed DFARS 252.204-7YYY(b)(1). This approach could affect contractors that were planning to establish separate information systems subject to separate CMMC requirements, such as one for handling FCI, another for handling CUI, and potentially even another for handling CUI of the type requiring Level 3 protection. It's not clear that DOD intended to prevent this multi-enclave approach, as DOD has also stated that it expects contractors to have, "on average 5 contractor information systems that will be used to process, store, or transmit FCI or CUI in performance of the contract."

Open Questions and Next Steps

In the August 15 proposed rule, DOD did not provide additional information in response to public comments on its December 2023 proposed rule regarding the CMMC cost analysis, DOD's assessment methodology under NIST 800-171, or the consistency of both proposed rules with other cybersecurity rules. For example, the August 15 proposed rule acknowledged the proliferation of component-unique cybersecurity rules within DOD but did not substantively address the issue or its effect on contractors trying to comply with multiple, potentially conflicting, requirements. Similarly, DOD made no attempt to harmonize the proposed DFARS requirements with cybersecurity requirements proposed or required by other agencies, including the U.S. Department of Homeland Security's Critical Infrastructure Security Agency and the FAR Council – ignoring Congress' and the Administration's plans for cybersecurity regulatory harmonization and creating another area of frustration for contractors.

We also anticipated that this rulemaking might provide DOD an opportunity to provide more guidance on issues that affect contractors more than government employees. For example, DOD could have more clearly articulated how it envisions prime contractors flowing down the CMMC 2.0 terms to subcontractors. But the new proposed rule offers little on the topic, deferring instead to the December 2023 proposed rule and to prime contractors. For example, DOD stated that it would be up to the prime contractor to determine which CMMC requirements would flow down to covered subcontracts based on the sensitivity of the unclassified information the subcontractors will receive and then obtain proof of that necessary CMMC certifications directly from each subcontractor annually. This limited guidance leaves open many questions for both prime and subcontractors.

DOD also missed a chance to more clearly articulate when information created or possessed by a contractor is done "for or on behalf of the Government." For contractors, this is a critical step to determining what constitutes CUI, but it is routinely ignored in Government policies and trainings, which are tailored to Government employees and do not provide contractors with necessary guidance. The latest proposed DFARS rule simply reproduced the existing CUI definition from Title 32.

The timing for implementation of a final DFARS rule on CMMC, which would start the three-year phase-in period, is still hazy. Before it can publish the final rule, DOD will have to review and respond to likely hundreds of comments on this proposed rule. DOD also cannot issue the DFARS final rule before it issues the Title 32

final rule, which will provide the substantive security requirements for contractors. DOD recently projected a final rule for Title 32 by November of this year, but those estimates have proven overly optimistic in the past. In addition, Congress will have an opportunity to review and possibly overturn any final rules under the Congressional Review Act, and the period for doing so could be extended under the Act's "lookback" provisions if there is a change in presidential administration.

Regardless of the timing, DOD appears to be marching forward with its plan to implement CMMC 2.0, and contractors should begin preparing if they have not already. Finally, civilian agency contractors that are not subject to CMMC should nonetheless familiarize themselves with its requirements because non-DOD agencies could elect to adopt CMMC for some or all of their contracts.

Wiley's cross-disciplinary Government Contracts, National Security, and Privacy, Cyber & Data Governance teams will continue to monitor these developments.