Westlaw Today
powered by Reuters

Department of Defense publishes long-awaited CMMC proposed rule

By Richard W. Arnholt, Esq., Adam Briscoe, Esq., and Todd R. Overman, Esq., Bass, Berry & Sims PLC*

JANUARY 23, 2024

On December 26, the Department of Defense (DoD) published its long-awaited Cybersecurity Maturity Model Certification (CMMC) Program proposed rule,[1] which places comprehensive cybersecurity and information security requirements on DoD contractors and subcontractors.

Currently, the DoD has a patchwork of security requirements implemented through various Defense Federal Acquisition Regulation Supplement (DFARS) clauses. However, it lacks a central tool to ensure contractors are continuously in compliance with those requirements. The proposed rule seeks to create a mechanism for the DoD to verify that sensitive unclassified information living on a contractor's information systems is protected with adequate and standardized safeguards.

Unlike the prior two levels, CMMC Level 3 imposes several additional security requirements to those under existing acquisition and procurement regulations.

With bated breath, federal contractors, government organizations, and other industry groups waited for this proposed rule for over two years following the DoD's abandonment of its initial vision for the CMMC Program (CMMC 1.0) and announcement of the "CMMC 2.0" Program in November 2021. The eventual final rule could result in the first phase of CMMC clauses being incorporated into DoD contracts as early as the first quarter of 2025. DoD and other interested parties are encouraged to submit comments to this proposed rule by February 26, 2024.

Applicability

The requirements of the proposed rule will apply to all DoD contracts and subcontracts where the awardees will process, store, or transmit information that meets the definitions of Federal Contractor Information (FCI) or Contractor Unclassified Information (CUI) on contractor-controlled information systems. The requirements will be implemented in DoD solicitations and contracts.

As previously released guidance has suggested, the CMMC program will consist of three levels.

CMMC Level 1

CMMC Level 1 is the most basic level of certification. In fact, many contractors already comply with the 15 security requirements under CMMC Level 1, given they mirror those required by Federal Acquisition Regulation (FAR) 52.204-21. CMMC Level 1 does not add any additional requirements on top of pre-existing obligations under FAR 52.204-21.

Contractors must annually self-certify, either through internal resources or engaging a third party, that these 15 requirements are implemented and enter the results in the Supplier Performance Risk System (SPRS).

A "senior official" from the prime contractor must initially "affirm" compliance with the 15 requirements and then also affirm continuing compliance with the specified security requirements on an annual basis thereafter. Contractors must submit the results of their self-assessment and the initial affirmation in SPRS prior to the award of any prime or subcontract and then on an annual basis after the award.

CMMC Level 2

Similar to CMMC Level 1, many contractors and subcontractors are already in compliance with CMMC Level 2 requirements. The requirements reflect the 110 security requirements under DFARS 252.204-7012, which is also aligned with National Institute of Standards and Technology (NIST) SP 800-171 Revision 2 requirements.

The proposed rule provides DoD Contracting Officers (COs) with discretion to determine whether CMMC Level 2 contracts should include a self-assessment requirement or only a CMMC Level 2 Certification Assessment to verify the implementation of the security requirements through a third-party certification organization. As stated in the proposed rule, the CO's decision will depend on the "program criticality, information sensitivity, and the severity of cyber threat."

Self-assessments for verifying CMMC Level 2 requirements are largely the same as those used for certifying CMMC Level 1 compliance. Contractors must submit the results of a self-assessment relating to its implementation of the NIST SP 800-171 Rev 2 requirements and an initial affirmation of

compliance from a "senior official from the prime contractor" to the SPRS system prior to award.

Additionally, if not all security requirements are already implemented, contractors seeking to obtain a CMMC Level 2 certification may have to submit a Plan of Action and Milestones Requirements (POA&M), a document that identifies tasks that need to be accomplished, resources required to accomplish the elements of the plan, milestones for meeting the tasks, and the scheduled completion dates for the milestones.

The proposed rule estimates that a Level 2 certification assessment will likely cost roughly $105,000 for a small entity and $118,000 for a large entity.

A CMMC Level 2 Certification Assessment requires contractors to engage an authorized or accredited CMMC third-party assessment organization (C3PAO) to certify compliance with the CMMC Level 2 security requirements.

The C3PAO will enter the results into the CMMC Enterprise Mission Assurance Support Service (eMASS), which will electronically transmit the assessment results into SPRS. Again, contractors must submit an initial affirmation of compliance, potentially a POA&M closeout affirmation, and then, on an annual basis, affirm its continuing compliance. A final certification is valid for up to three years.

CMMC Level 3

Unlike the prior two levels, CMMC Level 3 imposes several additional security requirements to those under existing acquisition and procurement regulations. Certification assessments for CMMC Level 3 are completed by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

Obtaining a CMMC Level 2 certification is a prerequisite to scheduling an assessment with the DIBCAC. DCMA's DIBCAC will perform the assessment and upload the results into eMASS, which will then feed them into SPRS.

Similar to the above, contractors are required to submit to SPRS an initial compliance affirmation, a POA&M closeout affirmation if applicable, and then, on an annual basis, submit an affirmation of continued compliance.

The CMMC level a contractor must meet will be detailed in each individual solicitation and contract. DoD program managers will determine which CMMC level is necessary based on a review of the type of information (FCI, CUI, etc.) that will be stored and processed through the contractor's information system throughout contract performance.

Rollout

The DoD will roll out the CMMC requirements over four phases. Phase 1, beginning on the effective date of the final rule, will require COs to include CMMC Level 1 Self-Assessment or Level 2 Self-Assessment requirements in all applicable DoD solicitations as a condition of contract award.

The proposed rule also allows DoD to make the successful completion of a self-assessment conditional to exercising a contract option period during Phase 1. Additionally, the proposed rule gives DoD discretion during Phase 1 to include CMMC Level 2 Certification Assessment instead of the Level 2 Self-Assessment for certain solicitations and contracts.

Phase 2 will begin the formal rollout of Level 2 Certification Assessments, and this requirement will be added to all applicable solicitations and contracts. The second phase will begin six months after the start of Phase 1. Similar to the discretion given to DoD in Phase 1, the proposed rule also gives DoD discretion to include the CMMC Level 3 certification assessment requirement in applicable solicitations and contracts.

One year after Phase 2 begins, Phase 3 will start. In Phase 3, the earnest implementation of the CMMC Level 3 Certification Assessment requirements for all applicable contracts will begin.

The proposed rule makes clear that CMMC compliance applies to narrow assessment scopes rather than entire organizations.

Lastly, Phase 4, beginning one calendar year after the start of Phase 3, will see DoD include CMMC program requirements in all applicable solicitations and contracts, including option periods for those awards made prior to Phase 4. The final and full rollout will likely come sometime in 2027.

Third-party certification process and costs

Under some solicitations rated as CMMC Level 2 and CMMC Level 3, the proposed rule requires contractors and applicable subcontractors to engage C3PAOs certified by DoD to verify compliance with the CMMC requirements and submit the assessment results via eMASS. This requirement will impose compliance costs on small and large businesses alike.

The proposed rule estimates that a Level 2 certification assessment will likely cost roughly $105,000 for a small entity and $118,000 for a large entity. CMMC Level 3 requires Level 2 compliance as a prerequisite but imposes additional recurring and nonrecurring engineering costs.

The proposed rule will likely make the defense industrial base more resilient against foreign actors seeking to steal national security secrets as well as intellectual property. However, the additional compliance costs on small and large defense contractors are inescapable. DoD has acknowledged outside of the proposed rule that the costs of CMMC compliance may be recoverable as an allowable cost for cost-type contracts.

But in the proposed rule, DoD specifically states that it "currently has no plans for separate reimbursement of costs to acquire

cybersecurity capabilities or a required cybersecurity certification that may be incurred by an offeror on a DoD contract."

Thus, contractors will likely be able to recover ongoing CMMC compliance costs following award through indirect costs, but there is no detailed procedure in the proposed rule, as drafted, for contractors to recoup pre-award costs incurred to meet CMMC contract eligibility requirements.

If the contractor and subcontractor are handling the same types of information, then the same CMMC-level certification will be necessary.

Accordingly, the rule places administrative and financial burdens on companies doing business with the government, which could prompt an exit from the defense industrial base for a variety of companies. On the other hand, compliance with these updated requirements could be seen as a competitive advantage and a sound investment in the future of a federal contracting business.

Assessment appeals

The proposed rule provides for a CMMC assessment appeals process for those contractors who disagree with a C3PAO's assessment results. The proposed rule requires C3PAOs to implement an internal "time-bound" appeals process to remedy disputes over potential malfeasance, unethical conduct, or other errors with the assessment. Appeals will first be reviewed and adjudicated by individuals uninvolved with the original assessment activities within the C3PAO.

A contractor may also request a copy of the certification organization's process. If both parties cannot resolve a dispute using the internal appeals process, it will be escalated to the Accreditation Body, an organization approved by DoD that will be responsible for accrediting third-party certifiers, which will have the authority to make a final decision.

Scope of organizational applicability

The proposed rule makes clear that CMMC compliance applies to narrow assessment scopes rather than entire organizations. Therefore, businesses with multiple business sectors may identify those sectors involved in the performance of the contract at issue and certify them in accordance with the applicable CMMC level.

A business may opt to certify one sector that will only handle FCI information against the CMMC Level 1 requirements while certifying another sector of the business at the CMMC Level 2 level because it will be supporting efforts requiring the higher level certification (i.e., handling CUI information).

The specific business units to be assessed, or boundaries of the assessment, must be identified by the contractor prior to the assessment.

Flow down requirements

As stated in the proposed rule, CMMC requirements "apply to prime contractors and subcontractors throughout the supply chain at all tiers that will process, store, or transmit FCI or CUI on contractor information systems in the performance of the contract or subcontract."

Prime contractors are required to flow down CMMC certification obligations to subcontractors at all tiers commensurate with the type and sensitivity of the information the subcontractors will process and/or handle.

For example, if a subcontractor will only process, store, or transmit FCI, then only CMMC Level 1 is required. But if a subcontractor will process, store, or transmit CUI in its scope of work, then a CMMC Level 2 Self-Assessment is required. If a subcontractor plans to process, store, or transmit CUI and the contract requires the prime contractor to obtain a Level 2 Certification Assessment, then the subcontractor must also obtain a Level 2 Certification Assessment.

Lastly, if a subcontractor plans to process, store, or transmit CUI in the performance of a contract where the prime contractor must obtain a Level 3 Certification Assessment, then the subcontractor is required to obtain a Level 2 Certification Assessment at minimum.

As drafted, the proposed rule does not clearly detail whether and under what circumstances a subcontractor would be required to undergo a Level 3 Certification Assessment.

In circumstances where the prime contractor only flows down certain information, a lower CMMC level may be appropriate. However, if the contractor and subcontractor are handling the same types of information, then the same CMMC-level certification will be necessary.

Conclusion

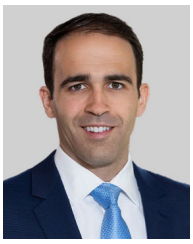
Following a long wait, the proposed rule gives contractors a detailed look into how the three-tiered certification program will operate. Given the complexity of the program and the number of comments that will likely be submitted in response to the proposed rule, we should not expect a final rule for a few months and potentially upwards of a year.

As a reminder, the comment period is open until February 26. Interested contractors who have questions on applicability or seek to shape the issuance of a final rule are encouraged to submit comments.

Notes

[1] https://bit.ly/3ObQGIi

About the authors


Richard W. Arnholt (L), a member at **Bass, Berry & Sims PLC** in Washington, D.C., advises government contractors on risk mitigation through ethics and compliance programs and on allegations of procurement fraud or misconduct. He can be reached at rarnholt@bassberry.com. **Adam Briscoe** (C), an associate at the firm in Washington, aids companies with federal, state and local government contracts. He can be reached at adam.briscoe@bassberry.com. **Todd R. Overman** (R) is a member of the firm, chair of its government contracts practice and managing partner of its Washington office. He counsels companies on government contracts, bid protests and litigation. He can be reached at toverman@bassberry.com. This article was originally published Jan. 3, 2024, on the firm's website. Republished with permission.

This article was published on Westlaw Today on January 23, 2024.