THOMSON REUTERS
Westlaw®

It's here! DoD issues interim rule launching two cyber assessment programs

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

NOVEMBER 16, 2020

For over a year, we have been discussing the Department of Defense's (DoD) eventual implementation of a Cybersecurity Maturity Model Certification (CMMC) program for Defense contractors, most recently during a webinar in September 2020 entitled CMMC is (Almost) Here! Latest Developments and Best Practices for Government Contractors[1].

The CMMC framework is part of DoD's efforts to enhance the protection of controlled unclassified information (CUI) within the federal supply chain.

In a move that surprised many observers, the interim rule requires that all contractors review their current cybersecurity compliance and report that status to the DoD for consideration before any new contract award, or before the DoD's exercise of any contract option.

On September 29, the Pentagon released an interim rule[2] under the Defense Federal Acquisition Regulation Supplement (DFARS) providing details on the implementation timeline of CMMC and the requirements defense contractors will have to adhere to starting November 30, 2020.

CMMC FIVE-YEAR ROLLOUT

The interim rule specifies that the CMMC program will be introduced in a five-year phased rollout that will be complete by September 30, 2025.

After that date, all defense contractors will be required to reach some level of CMMC certification if they are to receive future DoD contracts and subcontracts, except for DoD acquisitions solely for commercially available off-the-shelf (COTS) items.

During the rollout, the Under Secretary of Defense for Acquisition and Sustainment (USD (A&S)) will determine and communicate to Contracting Officers which contracts will require contractors to undergo a full third-party CMMC assessment.

So does this mean that defense contractors not bidding on contracts that require a third-party CMMC assessment are unaffected by the interim rule during the rollout? No.

In a move that surprised many observers, the interim rule requires that all contractors review their current cybersecurity compliance and report that status to the DoD for consideration before any new contract award, or before the DoD's exercise of any contract option.

DFARS CLAUSES IN PLACE DURING INTERIM

Specifically, the interim rule proposes two new DFARS clauses to be used between now and September 30, 2025, when all DoD contracts will need to be CMMC certified.

The first clause (DFARS 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement) is to be used in DoD contracts that need immediate CMMC certification through a third-party assessment.

As previously mentioned, the USD (A&S) will determine which contracts will require this over the next five years.

The second DFARS clause (DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements) applies to all DoD contracts (except COTS) during the five-year rollout.

Under this clause, contractors must report their compliance with NIST SP 800-171 security requirements on the DoD's Supplier Performance Risk System (SPRS)[3] and verify that the assessment is current (not more than three years old, unless a lesser time is specified in the solicitation).

The three levels of assessment are as follows: basic, medium and high.

- Basic — a self-assessment by the contractor and results in a confidence level of "low" since the contractor is self-reporting.
- Medium and high — assessments performed by the Defense Contract Management Agency (DCMA) and result in confidence levels of "medium" and "high," respectively.

Additionally, prime contractors cannot award subcontracts unless the subcontractor has also submitted its assessment of its compliance with NIST SP 800-171 security requirements to the DoD.

QUESTIONS REMAIN ABOUT INTERIM RULE

Despite the broad scope of the interim rule, significant basic questions still remain.

For example, the interim rule provides no definition of CUI and does not explain how Contracting Officers determine when a project requires that a contractor have a medium or high assessment, as opposed to basic.

> There is also no information on whether contractors face liability for an incorrectly conducted or reported self-assessment or assessment of a subcontractor.

Additionally, it is unclear if subcontractors must have the same level of assessment as the prime contractor, or if a basic assessment is sufficient for subcontractors.

There is also no information on whether contractors face liability for an incorrectly conducted or reported self-assessment or assessment of a subcontractor.

And while contractors can submit additional information up to 14 days after DCMA completes a medium or high assessment, there are no details on the form or process for challenging a DCMA assessment. It is also unclear how assessments will affect competition for contracts.

If a project requires a medium assessment, will a contractor with a high assessment have a better chance of securing the contract than a contractor with a medium assessment? Finally, how will these assessments factor into bid protests?

While the above questions remain, defense contractors should consider now whether to conduct a basic self-assessment, obtain a medium or high assessment by the DoD, or obtain a full third-party CMMC compliance assessment to avoid the risk of losing out on future opportunities.

If you have further questions or need assistance determining which course is right for you moving forward, please contact Richard Arnholt[4] or Todd Overman[5] or any member of our Government Contracts Practice Group[6].

Notes

1 https://bit.ly/3k1wmr4

2 https://bit.ly/34UUojl

3 https://bit.ly/3l09xoW

4 https://bit.ly/2I8BqwS

5 https://bit.ly/38b3ri1

6 https://bit.ly/32crQ39

This article was published on Westlaw Today on November 16, 2020.

ABOUT THE AUTHORS

Todd R. Overman (L) is a member at **Bass, Berry & Sims**, where he represents businesses throughout the contracting process with federal and state governments. He provides regulatory and compliance advice, M&A support, and litigation and dispute resolution. He can reached at TOverman@bassberry.com. **Richard W. Arnholt** (R), also a firm member, advises companies in contracting with federal and state governments. He mitigates risk through implementing ethics and compliance programs and responds to government allegations of procurement fraud or misconduct. He can be reached at rarnholt@bassberry.com. Both authors are based in Washington, D.C. This article was originally published Oct. 5, 2020, on the Bass, Berry & Sims firm website. Republished with permission.