# DOD REVAMPS CONTRACTOR CYBERSECURITY REQUIREMENTS WITH CMMC 2.0

Date: 11 November 2021

**U.S. Policy and Regulatory Alert**

By: Erica L. Bakies, Amy C. Hoang, Sarah F. Burgart

On 4 November 2021, the Department of Defense (DoD) announced “CMMC 2.0,” a planned revamp of the Cybersecurity Maturity Model Certification (CMMC) framework. Here are the key takeaways:

- CMMC 2.0 creates three levels of cybersecurity maturity (as opposed to the five levels in CMMC 1.0).
- For Level 1 and some Level 2 assessments, contractors may self-certify compliance rather than using third-party assessors.
- DoD is suspending the current CMMC 1.0 pilot until it implements CMMC 2.0 through formal rulemaking.
- Like CMMC 1.0, the revamped requirements will apply to both prime contractors and their lower-tier subcontractors.

## OVERVIEW

CMMC 2.0 follows an interim Defense Federal Acquisition Regulation Supplement (DFARS) rule released on 29 September 2020, which planned for all defense contracts to incorporate the robust requirements of CMMC 1.0 by FY 2026 (see our summary of the previous CMMC 1.0 framework here). After reviewing comments on the interim rule from industry and other stakeholders, DoD announced the CMMC 2.0 changes to the framework last week. With these changes, DoD steps back from many of the CMMC 1.0 requirements that previously defined the framework. This alert summarizes the key changes announced with CMMC 2.0, the updated timeline contractors can expect for CMMC implementation, and CMMC resources that contractors can expect to see from DoD going forward.

## KEY CHANGES FROM CMMC 1.0 TO CMMC 2.0

### Reduction of Certification Levels

CMMC 2.0 reduces the framework from five certification levels to three. CMMC 2.0 eliminates Level 2 and Level 4 in alignment with previous DoD statements that Levels 2 and 4 were merely transition levels to their respective higher levels of maturity. The levels will be renamed to Level 1, Foundational (previously Level 1); Level 2, Advanced (previously Level 3); and Level 3, Expert (previously Level 5).

### Self-Assessments and Government-Led Assessments

The most dramatic shift planned for CMMC 2.0 is removal of the requirement that all certification assessments be performed by third-party organizations, dubbed CMMC Third-Party Assessment Organizations (C3PAOs).

Under the updated framework, Level 1 certification and certain nonprioritized acquisitions assigned Level 2 will require only an annual self-assessment and accompanying contractor affirmation in the Supplier Performance Risk System (SPRS). Prioritized acquisitions assigned Level 2 will require the previously anticipated C3PAO assessments every three years. All certifications at Level 3 will require a government (rather than C3PAO) assessment every three years.

These updates demonstrate both a step back from the requirement that independent organizations conduct all assessments and a step toward the government being more involved in the CMMC assessment process. DoD announced that it will require both the CMMC Accreditation Body (CMMC AB, the entity previously charged with full implementation of the assessment process) and C3PAOs to achieve enhanced professional and ethical standards before completing assessments under the CMMC 2.0 framework.

### Limited POAMs

Under certain circumstances, CMMC 2.0 will allow contractors to implement time-limited Plans of Action and Milestones (POAMs) in order to achieve full certification. DoD will specify an absolute number of cybersecurity requirements that must be achieved prior to contract award, as well as a small set of critical requirements that must always be achieved prior to award and which may not appear in a contractor's POAM. The allowance for a POAM, even if limited, is a significant change from the prior model, which required that contractors achieve the applicable CMMC level certification to even be eligible to receive a defense contract award.

### Limited Waivers

Under certain limited circumstances for select mission critical acquisitions, CMMC 2.0 will allow contractors to obtain waivers of CMMC requirements. Waivers must be approved by DoD senior leadership and will be time-limited. Again, even with limitations, a CMMC waiver process is a large shift from the previous model, where certification was a “go/no-go” criterion for receiving a defense contract award.

### Streamlined Practices

CMMC 2.0 draws only from the National Institute of Standards and Technology Special Publication (NIST SP) 800-171 and NIST SP 800-172 to create its cybersecurity standards. It no longer contains any cybersecurity practices drafted specifically for the CMMC framework or practices pulled from various domestic and international cybersecurity standards.

### Removal of Maturity Processes

CMMC 1.0 proposed to evaluate both cybersecurity processes and cybersecurity practices. Practices evaluated technical activities required for certification, whereas processes evaluated the extent of institutionalization of those practices. CMMC 2.0 eliminates the concept of maturity processes and contains only the cybersecurity practices themselves.

## CMMC 2.0 IMPLEMENTATION TIMELINE

DoD intends to implement CMMC 2.0 through notice-and-comment rulemaking to be codified in CFR Chapters 32 (National Defense) and 48 (DFARS). Until rulemaking for each of these chapters is complete, DoD is suspending its CMMC piloting efforts and will not include CMMC requirements in any contracts. The CMMC website states that the rulemaking process can take anywhere from nine to 24 months, meaning that the earliest DoD expects to implement CMMC requirements is August 2022. At the same time, DoD is considering providing incentives to contractors who achieve CMMC certification while rulemaking is underway.

## DOD RESOURCES FOR CMMC 2.0

As with previously released iterations of the CMMC framework, DoD is intending to provide the full model for Levels 1 and 2, as well as Assessment Guides for each level, in coming weeks on the CMMC website. Level 3 is still under development but will be posted when available. DoD has also provided an FAQ page to address initial questions regarding CMMC applicability, requirements, assessments, and implementation.

Additionally, DoD has developed Project Spectrum, a cybersecurity resource platform to assist contractors with assessing and enhancing their cybersecurity practices. Project Spectrum provides multiple resources, including blogs, white papers, courses, videos, and other information on various aspects of cybersecurity. Although DoD is suspending implementation of CMMC requirements until CMMC 2.0 is fully codified, DoD is encouraging contractors to continue assessing and updating their cyber capabilities.

Finally, DoD is developing a set of acceptance standards between certain existing cybersecurity frameworks and CMMC requirements, including for GSA's FedRAMP and the NIST SP 800-171 DoD Assessment Methodology. Further guidance will be provided regarding potential CMMC reciprocity for these standards once developed.

## CONCLUSION

The release of CMMC 2.0 demonstrates a significant revamp of the CMMC framework, with DoD relaxing some of the strict assessment and compliance requirements that defined the last iteration of the model. However, CMMC 2.0 indicates that DoD has a defined plan for moving forward with full implementation of its revised framework, and contractors should not expect to see CMMC disappear anytime soon.

The K&L Gates Government Contracts and Procurement Policy group can help your company navigate CMMC basics and assess how CMMC 2.0 will impact cybersecurity obligations under federal contracts. We will continue to monitor the CMMC implementation and requirements as DoD begins the rulemaking process.

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.