wiley

ALERT

Cyber Developments: DOD Suspends CMMC Version 1.0 and Charts a New Course With "CMMC 2.0"

November 5, 2021

WHAT: On November 4, 2021, the U.S. Department of Defense (DOD) announced the completion of a months-long internal review and significant changes to the strategic direction of its Cybersecurity Maturity Model Certification (CMMC) program, culminating with "CMMC 2.0." Several elements are unsettled as of this writing. But one piece is clear: the original concept of CMMC has been radically altered.

DOD described many of the key changes in an Advanced Notice of Proposed Rulemaking (ANPRM) that was temporarily available for public inspection on the Federal Register's website and in a revised website for CMMC 2.0. Until DOD completes a new rulemaking process, it is suspending CMMC pilot efforts and will not include CMMC requirements in new solicitations. Although DOD will call its next effort "CMMC 2.0," that effort will abandon many of the controversial aspects of CMMC, including the maturity processes, prohibitions on plans of action and milestones (POAMs), and, in some cases, even the need for certifications from independent third parties. Instead, CMMC 2.0 will consist of three levels; require security practices aligned with National Institute of Standards and Technology (NIST) 800-171 and 800-172; and rely on a mix of self-attestation, third-party assessment, and Government assessment.

WHEN: DOD will implement these changes through a forthcoming rulemaking process, which DOD anticipates taking 9-24 months. This rulemaking will amend Title 32 of the Code of Federal Regulations (C. F.R.) and the Defense Federal Acquisition Regulation Supplement (DFARS) in Title 48 of the C.F.R. Both rules will have a public comment

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Practice Areas

Cybersecurity
Government Contracts
Privacy, Cyber & Data Governance

period.

WHAT DOES IT MEAN FOR INDUSTRY: This announcement relieves contractors from the imminent need to prepare for CMMC requirements, at least in their current form. This means contractors can focus on ensuring compliance with existing cybersecurity requirements, including DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting and DFARS 252.204-7020, NIST SP 800-171 DOD Assessment Requirements.

Shortly after making it available for public inspection, DOD withdrew the ANPRM, which suggests at least the potential for some uncertainty here. However, DOD also highlighted many of these same changes on the new CMMC 2.0 website, which remains available. Together, these documents show that DOD intends to make several significant changes to the CMMC Model during this new rulemaking process. Here are the most significant changes:

No Maturity Processes: The first *M* in CMMC stood for *Maturity*. In addition to data security controls, the CMMC Model sought to evaluate the maturity of a contractor's implementation of cybersecurity practices by requiring additional "maturity processes." DOD appears to be moving away from this approach and eliminating maturity processes.

No CMMC-Unique Practices: CMMC 1.0 differed from other cybersecurity regimes, such as NIST SP 800-171, because it included requirements not found in other publications. DOD is removing CMMC-unique practices. That means CMMC 2.0 will rely entirely on security practices prescribed in other publications, including NIST SP 800-171 and SP 800-172.

Plans of Action & Milestones (POAMs) Allowed: CMMC 1.0 also differed from other cybersecurity regimes because it required a contractor to implement 100% of all security practices to be considered compliant. Other regimes such as DFARS 252.204-7012 and NIST SP 800-171, by contrast, considered a company compliant if the company developed a plan of action to correct any deficiencies or implement any missing controls. DOD plans to return to a more flexible approach using "a time-bound and enforceable Plan of Action and Milestone process." With these announcements, DOD also previewed a "selective, time-bound waiver process." The details of when POAMs and waivers will be allowed are unknown and will be critical for contractor compliance when CMMC 2.0 is implemented.

Self-Assessments Allowed: CMMC 1.0 was also unique because it required contractors to undergo a third-party assessment and certification. As discussed more below, DOD is limiting this requirement. Self-assessments will be allowed for many contractors, depending on the CMMC level required in a contract and whether the contract involves information critical to national security.

Fewer Levels: The CMMC Model previously included five levels with varied requirements. The new program will now include just three levels. The summary below identifies our understanding of DOD's plans for these three levels:

- **Foundational/Level 1 (previous level 1):** Level 1 will likely apply to companies that process, store, or handle Federal Contract Information. For this level, DOD intends to allow companies to perform self-assessments. This level will require companies to comply with a limited subset of NIST SP 800-171 controls.
- **Advanced/Level 2 (previous level 3):** Level 2 will likely apply to companies that process, store, or transmit Controlled Unclassified Information (CUI). If the contract also involves information critical to national security, DOD will require the contractor to obtain a third-party assessment from an organization accredited by the CMMC Accreditation Body; otherwise, DOD will allow the company to perform a self-assessment. Level 2 will be equivalent to NIST SP 800-171.
- **Expert/Level 3 (previous level 5):** Level 3 will be based on a subset of NIST 800-172 requirements and will likely require an assessment conducted by government officials. These assessment requirements are currently under development.

There is still a lot to be determined. At this point, however, CMMC 2.0 looks likely to resemble the original CMMC program in name only. Instead, it looks much more like DOD's current status quo. In particular, the move to at least some self-assessments and elimination of CMMC-unique practices mirrors the existing NIST SP 800-171 Assessment Methodology, which DOD rolled out alongside the CMMC program last September. That program requires contractors to assess their own compliance with NIST 800-171 and attest to their compliance while also reserving for DOD the right to evaluate the contractor's compliance, if needed.

DOD estimated that the rulemaking process for CMMC 2.0 can take "9-24 months," and the CMMC 2.0 will not be a contract requirement until after that is complete. In the meantime, DOD contractors may need to reassess their ongoing planning for CMMC in light of these announced changes. In addition, contractors need to focus on their existing data security requirements, especially contracts that require meeting the security controls in NIST 800-171.