wiley

NEWSLETTER

What Contractors Need to Know About DoD's New CMMC Program

March 2020

Privacy in Focus®

The U.S. Department of Defense (DoD) is in the process of establishing a new cybersecurity program for the Defense Industrial Base (DIB): the Cybersecurity Maturity Model Certification (CMMC). While DIB contractors already must comply with burdensome cybersecurity requirements, the CMMC represents a fundamental change in approach. Once fully implemented, the CMMC will require *all* DoD contractors and subcontractors to obtain a third-party cybersecurity certification in order to compete for defense contracts. This fundamental change is happening at a breakneck pace: DoD announced this new program in June 2019, released version 1.0 of the CMMC framework at the end of January 2020, launched the rulemaking process to update the Defense Federal Acquisition Regulation Supplement (DFARs) in January 2020, and reportedly hopes to start including CMMC requirements in at least some Requests for Information (RFIs) and solicitations this year, with expected growth of the program over the next several years.

Given the scope of this development, and the speed at which it is being implemented, it is critical that DoD contractors and subcontractors stay up to date on the process and are prepared to meet the new certification expectations. This article details the most important updates thus far in the process to stand up the CMMC, explaining how the CMMC compares to current cybersecurity expectations and what contractors should do to prepare.

As Currently Planned, the CMMC Will Require Third-Party Cybersecurity Certification for All DoD Contractors and Subcontractors

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Practice Areas

Government Contracts

Privacy, Cyber & Data Governance

Telecom, Media & Technology

White Collar Defense & Government Investigations

The focus of the CMMC is to protect two main categories of unclassified information: federal contract information (FCI) and controlled unclassified information (CUI**)**. To do this, the CMMC framework creates five levels of certification, each measuring increasing levels of cybersecurity maturity. Levels 1 and 3 generally track to current cybersecurity expectations. **Level 1** is roughly equivalent to the basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.201-21, which is included in civilian contracts. **Level 3** will generally be intended for contractors who are processing CUI and is roughly equivalent to the current security requirements for protecting CUI in NIST SP 800-171, although there are significant differences. Most notably, Level 3 requires implementation of a total of 20 additional practices beyond NIST SP 800-171 that are derived from a variety of other sources. **Levels 4 and 5** add additional practices from these bases, some of which are consistent with draft NIST 800-171B, which seeks to protect CUI at a "higher than usual risk of exposure," including from Advanced Persistent Threats (APTs).

As illustrated by DoD, the reach or focus of each level is as follows:

Level 1:

Safeguard Federal Contract Information (FCI)

Level 2:

Serve as transition step in cybersecurity maturity progression to protect CUI

Level 3:

Protect Controlled Unclassified Information (CUI)

Levels 4-5:

Protect CUI and reduce risk of APTs

Importantly, DoD expects that "all companies doing business with the Department of Defense will need to obtain CMMC" certification, including all contractors and subcontractors. That is a change from the current regime, which only requires contractors that process CUI in support of the performance of a DoD contract to meet the heightened cyber requirements in NIST SP 800-171.

The CMMC Builds From – But Is Fundamentally Different Than – Current Cybersecurity Requirements and the FedRAMP Program

The CMMC builds on existing cybersecurity requirements. As it stands, many defense contractors must already comply with the requirements of DFARS 252.204-7012 and NIST SP 800-171 – and, as noted above, fully satisfying these requirements enables a contractor to approximate that it could achieve a CMMC Level 3 certification. However, the CMMC program represents a fundamental shift in approach in that it adds a requirement for contractors to be certified at a given level by an independent third-party assessing official. As DoD explains, the CMMC "add[s] a verification component with respect to cybersecurity requirements," in

contrast to the existing regime, which is "based on trust" and self-verification of compliance.

The CMMC's model of independent third-party certification bears some resemblance to the Federal Risk and Authorization Management Program (FedRAMP). As with FedRAMP, contractors will be required to achieve incremental levels of certification by an independent organization. However, the potential scope of companies that may require CMMC certification is significantly broader than the FedRAMP program, which only applies to the relatively smaller number of companies that provide cloud services to the federal government.

DoD Will Rely on an Independent Accreditation Body to Implement Its Third-Party Certification Program

DoD has decided to task the private sector, in coordination with academia, with standing up an Accreditation Body (AB) which will be tasked with training and certification of the CMMC Third Party Accreditation Organizations (C3PAOs) responsible for certifying the entire DIB. Private-sector actors will thus have the responsibility to certify DoD contractors so that they can participate in and compete for DoD awards beginning in late 2020.

Notably, there have been some delays in establishing the AB. DoD originally anticipated having the AB sign a Memorandum of Understanding (MOU) with DoD to formalize the AB's authority and functions in early December 2019, but that deadline has already slipped. Recent reports indicate that DoD and the AB will sign the MOU in March 2020. Nonetheless, the AB has elected a Board of Directors consisting of 14 individuals and is currently seeking industry input on a range of questions, including the appropriate cost for CMMC certification. The AB is also reportedly planning to conduct its first training of C3PAOs in Spring 2020.

The AB's progress is critical for implementation of the CMMC regime because C3PAOs and individual assessors will not be able to receive training and certification until the AB is established. In turn, contractors will be unable to become certified until there are a sufficient number of C3PAOs authorized to conduct certifications.

DoD Has an Aggressive Timeline for CMMC

DoD has continued to advance an aggressive timeline for the CMMC. Initially, DoD stated that Requests for Information (RFIs) would begin to include CMMC levels in June 2020 and solicitations begin to include CMMC levels shortly thereafter. This would seem to have required certification broadly across the DIB, consisting of more than 300,000 contractors, by sometime this year. As challenges with this schedule became apparent, including delays in standing up the AB, DoD appears to have narrowed the scope for the CMMC this year. It has been reported that DoD plans to include CMMC requirements in approximately 10 solicitations this year and aims for 1,500 contractors to be certified in 2021, 7,500 more to be certified in 2022, and 25,000 more to be certified in 2023. DoD has stated that it will take several years until the entire DIB is certified to at least some CMMC level.

How Should DoD Contractors Prepare for the New CMMC?

Contractors and other stakeholders can engage with DoD as it is establishing this new program. One key opportunity for engagement will be DoD's CMMC rulemaking, which was initiated in January. Specifically, DoD is drafting a proposed DFARS rule that will contractually implement the CMMC requirements. DoD's utilization of the rulemaking process will provide industry the opportunity to formally provide input and comment on the impact of the proposed rule, which DoD is hoping to finalize by September 2020. Given the volume and intensity of industry feedback throughout the development of the CMMC, it is likely that DoD will be inundated by comments, which may further delay the issuance of a finalized rule.

As the CMMC program develops, contractors may wish to consider the additional practices and processes necessary to demonstrate compliance with a given CMMC Level, as there may be little time to achieve certification in time for an acquisition once the minimum level is announced in a solicitation. For now, however, speculating about which CMMC Levels may be required for a specific contract may be little more than educated guessing. In most cases, contractors will likely want to hold off on major investments to meet a specific CMMC Level until DoD has established greater clarity. That said, DFARS 252.204-7012 and NIST SP 800-171 are still contractual requirements and DoD has indicated they will remain so during the multi-year transition to CMMC. For covered contractors, ensuring appropriate compliance with the DFARS requirements may be a more pressing need.

Contractors should pay close attention to the rapidly developing CMMC requirements and policies announced by DoD, the Accreditation Body, and other stakeholders. As the CMMC is deployed, there may be opportunities for constructive engagement with DoD and to anticipate future cyber obligations.