wiley

ALERT

DOD Releases Draft of the Cybersecurity Maturity Model Certification (CMMC) Plan; Industry Input Sought

September 11, 2019

WHAT: DOD announced the much-anticipated first public draft of the anticipated Cybersecurity Maturity Model Certification (CMMC) Model, draft CMMC v0.4. DOD's CMMC promises to be a substantial addition to the regulatory and compliance burden faced by contractors, and the newly issued draft CMMC v0.4 provides additional detail regarding the specific controls required under the CMMC Model.

WHEN: Comments are due September 25, 2019.

WHAT DOES IT MEAN FOR INDUSTRY: DOD is seeking input from industry to prioritize the cybersecurity controls which will be required to obtain certification under the CMMC Model. Contractors will be required to be certified to various CMMC Levels in order to be eligible for award of DOD contracts, so this is a critical opportunity to engage with DOD.

CMMC Overview

Under the proposed CMMC process, a DOD contractor's cyber maturity will be certified by independent accredited third-party organizations. The CMMC framework includes five maturity "Levels," with Level 1 setting out the most basic cyber hygiene, and Level 5 the most advanced. Starting in Fall 2020, DOD solicitations will specify the CMMC Level which contractors will be required to meet as a "go / no go" decision point for contract awards.

The controls for each CMMC level are based on a variety of sources,

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Jon W. Burd
Partner
202.719.7172
jburd@wiley.law

Practice Areas

Government Contracts

Privacy, Cyber & Data Governance

including NIST SP 800-171, other data security regimes, like ISO 27001 and CIS Critical Security Controls 7.1, as well as other "best practices."

- At the low end, CMMC Level 1 is considered "basic cybersecurity." Level 1 includes a relatively small subset of data controls from NIST SP 800-171, the FAR Basic Safeguarding Clause 52.204-21, and other practices.
- Level 3 most closely approximates what is currently required by DFARS 252.204-7012 and NIST SP 800-171. CMMC Level 3 includes "all" NIST SP 800-171 rev 1 controls plus "additional practices beyond the scope of CUI protection."
- At the high end, CMMC Level 5 includes all of NIST SP 800-171, plus significant additional controls like real-time asset tracking, autonomous initial response actions, network segmentation, and a 24x7 Security Operations Center (SOC). CMMC Level 5 is considered to require "highly advanced cybersecurity practices."

CMMC v0.4 provides a detailed matrix of the numerous controls required at each maturity Level. However, DOD made clear that these controls are still being "refined," and it appears likely that significant changes to the controls will occur in subsequent revisions.

Schedule

Comments on the first draft of the CMMC Model are due on September 25, 2019. DOD envisions a second round of comments in November 2019, and release of the final version in January 2020. DOD plans to use the CMMC Model in RFIs in June 2020 and in RFPs in Fall 2020.

The Relationship Between CMMC and DFARS 252.204-7012 is Not Clear

DOD states that "[t]he CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements." There is no indication thus far that DOD intends for CMMC to replace or amend DFARS 252.204-7012. Rather, CMMC and DFARS 252.204-7012 will operate independently of each other. Of note, **DOD stated that CMMC certification will apply to all DOD contractors, including subcontractors—and even those that do not process CDI**. *See* DOD FAQ Question #20-#21 ("All companies conducting business with the DOD must be certified. The level of certification required depends upon the CUI a company handles or processes."). This raises challenging questions about whether and how contractors must meet the DFARS' requirements and be certified under CMMC.

Relatedly, there does not appear to be a clear correlation between CMMC Levels 4 and 5 and draft NIST SP 800-171B (released in June 2019). Draft NIST 800-171B recommends the implementation of 32 enhanced security requirements in addition to the 110 requirements listed in NIST SP 800-171. It does not appear, however, that the controls required under CMMC Levels 4 and 5 are coextensive with the requirements in NIST SP 800-171B. Further, draft NIST SP 800-171B, purports to only apply to "critical programs" and "high value assets." In some ways, this appears to correspond to CMMC Levels 4 and 5, which are targeted towards "a small subset" of systems that "support DOD critical programs and technologies." However, NIST SP 800-171B lacks a definition for "critical programs" or "high value assets," so it is uncertain to what degree contractors required to meet NIST SP 800-171B must also be certified to CMMC Levels 4 or 5.

In addition, CMMC does not appear to address some of the most challenging scope questions arising under DFARS 252.204-7012. Most notably, CMMC does not appear to provide clarity on the second part of the definition of CDI, or 'unmarked CDI.' *See* DFARS 252.204-7012(a) (CDI includes CUI that is, "Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract."). The CMMC also does not clarify what constitutes an information system boundary, which causes uncertainty for contractors trying to determine the scope of information systems that must comply with DFARS 252.204-7012.

Perfect Compliance May Not Always Be Required

DOD acknowledged "the challenges of being 100% compliant with some [CMMC] practices." For example, it may be impractical for an entity with thousands of end points to always maintain a perfect, up-to-date asset inventory. DOD thus suggests that "policies, plans, processes, and procedures" can "offset the need for 100% compliance for some practices." The idea appears to be that a proper policy and process institutionalization regarding asset inventory may be sufficient to obtain CMMC certification, even where there are minor instances in which not all devices are inventoried. Though it is unclear how this would work in practice, industry will likely welcome DOD's apparent openness to the notion that perfect compliance may be offset with mature cyber policies and procedures.

Request for Feedback

DOD has requested comments on the current draft by September 25, 2019. In particular, DOD listed the following specific questions on which it is seeking comments:

1. What do you recommend removing or de-prioritizing to simplify the model and why?
2. Which elements provide high value to your organization?
3. Which practices would you move or cross reference between levels or domains?
4. In preparation for the pending easy-to-use assessment guidance, what recommendations might you have to clarify practices and processes?

We will be monitoring this as DOD releases new details.