wiley

NEWSLETTER

Cybersecurity Updates: What We've Learned About CMMC 2.0 So Far

April 2022

Last November, the U.S. Department of Defense (DOD) announced sweeping changes to the Cybersecurity Maturity Model Certification (CMMC) program in a new "version 2.0." Although we are still awaiting the interim regulations, which DOD plans to release by May 2023, DOD has revealed several updates over the last few months.

We summarized the most significant changes for contractors to anticipate last November, when DOD announced CMMC 2.0:

- DOD plans to eliminate the maturity processes entirely (which had represented the first "M" in CMMC).
- DOD plans to remove all CMMC-unique practices, meaning CMMC 2.0 will rely entirely on security practices prescribed in other publications, including National Institute of Standards and Technology (NIST) SP 800-171 and SP 800-172.
- DOD will allow for some flexibility with limited, time-bound Plans of Action and Milestones (POAMs) to implement outstanding controls.
- DOD will allow some contractors to conduct self-assessments and will conduct some assessments itself using government personnel.
- DOD intends to reduce the model from five levels to three:
    - 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.

Authors

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Cybersecurity

Government Contracts

Privacy, Cyber & Data Governance

- Advanced/Level 2 (previous level 3): Level 2 will likely apply to companies that process, store, or transmit Controlled Unclassified Information (CUI). DOD anticipates two sub-levels. 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 (DIBCAC).

Following this announcement, in December 2020, DOD released two sets of guidance documents. The first set, referred to as **Scoping Guidance**, is significant because it articulates what the contractor (or the assessor) needs to evaluate for compliance at a more nuanced level than the current Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 clause. Currently, the -7012 clause requires contractors to provide adequate security for "information systems" that process, store, or transmit covered defense information. The clause then defines "information system" as "a discrete set of information resources . . . ." This leaves room for debate over what is part of a covered information system and where the information system boundaries lie.

The Level 2 Scoping Guidance provides additional nuance by establishing a two-step asset-specific framework. In the first step, contractors can exclude from the assessment scope any assets that (1) do not themselves process, store, or transmit CUI and (2) are physically or logically separated from those that do. In the second step, contractors determine which requirements apply to the remaining in-scope assets. At a minimum, contractors will be required to document all in-scope assets in the asset inventory and System Security Plan (SSP). But the remaining requirements vary depending on the type of asset. The Level 2 Scoping Guidance describes four categories of assets:

- **CUI Assets** are assets that process, store, or transmit CUI. Contractors must assess these assets against all CMMC practices.
- **Security Protection Assets** are assets that provide security functions or capabilities to the contractor's CUI assets, regardless of whether they process, store, or transmit CUI themselves. Contractors must assess these assets against all CMMC practices as well.
- **Contractor Risk Managed Assets** are assets that theoretically can process, store, or transmit CUI because they are not physically or logically separated, but they are not intended to do so based on the contractor's security policies, procedures, and practices in place. Contractors do not need to assess these assets against all CMMC practices. Instead, contractors may apply risk-based security policies, procedures, and practices.
- **Specialized Assets** are assets that also may process, store, or transmit CUI but also fall into one of the following categories: government property, Internet of Things (IoT) devices, Operational Technology (OT), Restricted Information Systems, and Test Equipment. Contractors do not need to assess these assets against all CMMC practices.

The second set of documents, referred to as **Assessment Guides**, provides additional discussion and examples for testing compliance with each of the security controls required. In addition to these documents, the CMMC Accreditation Board is also working to finalize its own CMMC Assessment Process (CAP) guide. That document is not yet available.

In early February, DOD also announced new leadership for the CMMC program. In particular, DOD transferred responsibility for the CMMC program from the Officer of the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) to the DOD Chief Information Officer (CIO). Deputy CIO for cybersecurity David McKeown will directly oversee the program going forward. Since this transfer, DOD has foreshadowed additional anticipated changes to the CMMC program. For example, although DOD initially announced a plan to bifurcate Level 2 depending on whether the CUI was "critical to national security," DOD representatives anticipate that most contractors with CUI will fall into the higher tier within Level 2 that will require a Certified Third Party Assessment Organization (C3PAO) assessment. Still, DOD expects to include a provision in the upcoming rulemaking that clarifies the distinction between the sublevels to help contractors identify whether CUI is "critical to national security." DOD is also exploring potential ways to promote early adoption of the requirements and early completion of assessments, even before the rulemakings take effect, but it is unclear what, if any, incentives DOD could provide.

DOD has also clarified that its previous CMMC-unique security controls may resurface. DOD still intends to rely solely on NIST SP 800-171 and SP 800-172 to define the required security controls for CMMC 2.0. But DOD intends to work with NIST to have NIST add controls to its publications. NIST has announced that it expects to update its controls this year, although it is not yet clear whether that will include the previous CMMC-unique controls.

Finally, although there is still some uncertainty about the timeline, in its latest comments DOD has expressed a desire to issue the interim rule implementing CMMC 2.0 by May 2023, with initial requirements showing up in DOD contracts 60 days after the interim rule publication. DOD is also working to finalize additional guidance for identifying CUI, which has been under development for just over 18 months.

In the meantime, DOD has been encouraging contractors to focus on compliance with the current requirements in the -7012 clause as well as the assessment requirements in DFARS 252.204-7019 and -7020, which DOD announced at the same time as CMMC 1.0 in September 2020. Although DOD is taking some time to retool CMMC 2.0, these other assessment requirements remain applicable now. DOD recently separated these assessment requirements into a separate DFARS Case (2022-D017) so that it can issue a final rule while it continues to refine its approach for CMMC 2.0. DOD also announced on March 29, 2022, that it will be initiating Medium Assessments under the -7020 clause in "a couple months." Under these Medium Assessments, the Defense Contract Management Agency (DCMA) will review a contractor's System Security Plan (SSP), supporting documents, and any previous Basic Assessments that the contractor self-generated.

We expect many more updates to come as DOD refines and rolls out its new CMMC 2.0, and we will continue to publish periodic summaries of any developments.