Updated: November 15, 2021

LEWIS-BURKE ASSOCIATES LLC

CMMC 2.0 Overview and Fact Sheet

This document provides an update on the CMMC 2.0 guidance released on November 4, 2021.

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a new framework of standards for cybersecurity practices across academic, industry, and other Defense Industrial Base (DIB) organizations that contract with and support the Department of Defense (DOD). The goal of CMMC is to enhance the protection of Controlled Unclassified Information (CUI) across the supply chain through a standard assessment model and framework for compliance, including a hierarchy of cybersecurity regulations and practices. DOD published an interim rule on September 29 in the federal register for how this framework would be implemented. In March 2021, the DOD conducted an internal assessment of the CMMC program based on the hundreds of public comments they received. That resulted in the update of the program structure in November 2021, creating CMMC 2.0.

Why did DOD establish CMMC?

The CMMC program was developed in response to concerns about cyberattacks against the contractors and organizations that support the DOD. DOD officials have discussed the potential for adversaries to hack contractors for a variety of purposes. This could include espionage or could also include other goals such as driving small defense contractors out of business or modifying requirements on a system to cause critical failures down the road. Due to previous findings that a significant number of contractors and subcontractors have not sufficiently complied with current cybersecurity standards requirements, the Department is establishing and implementing the CMMC framework to better protect the DIB.

How does CMMC work?

The CMMC 2.0 framework has three levels of requirements and processes that organizations must implement to ensure the security and protection of CUI related to a DOD-funded project. The CMMC Accreditation Body (CMMC-AB), working alongside DOD, has created the requirements for organizations to be CMMC certified and is currently commissioning Third Party Assessment Organizations (C3PAOs) C3PAOs to conduct CMMC assessments and certify CMMC certifications. The C3PAOs will be tasked with conducting assessments on Level 2 and 3 contractors. As of November 2021, the three levels are as follows:

- Level 1: Foundational
- Level 2: Advanced
- Level 3: Expert

Organizations applying for grants or contracts from the Department will have to have the appropriate CMMC level specified in that grant or solicitation at the time of award. In most cases, fundamental research would require CMMC level 1, which would ensure basic cyber hygiene practices such as monitoring and limiting access to operating environments (laboratories) and information systems;

scanning systems for and maintaining updated systems to protect against malicious code; and limiting data access from DOD-sponsored projects to authorized users.

CMMC Level 2 requires adoption of the National Institutes of Standards and Technology's (NIST) standards for protecting CUI, known as Special Publication (SP) 800-171 Rev. 1. Level 2 includes a subset that involves information critical to national security which will require an assessment by a C3PAO. The other subset of level 2 would not involve information critical to national security, and associated contractors will only be required to conduct self-assessments.

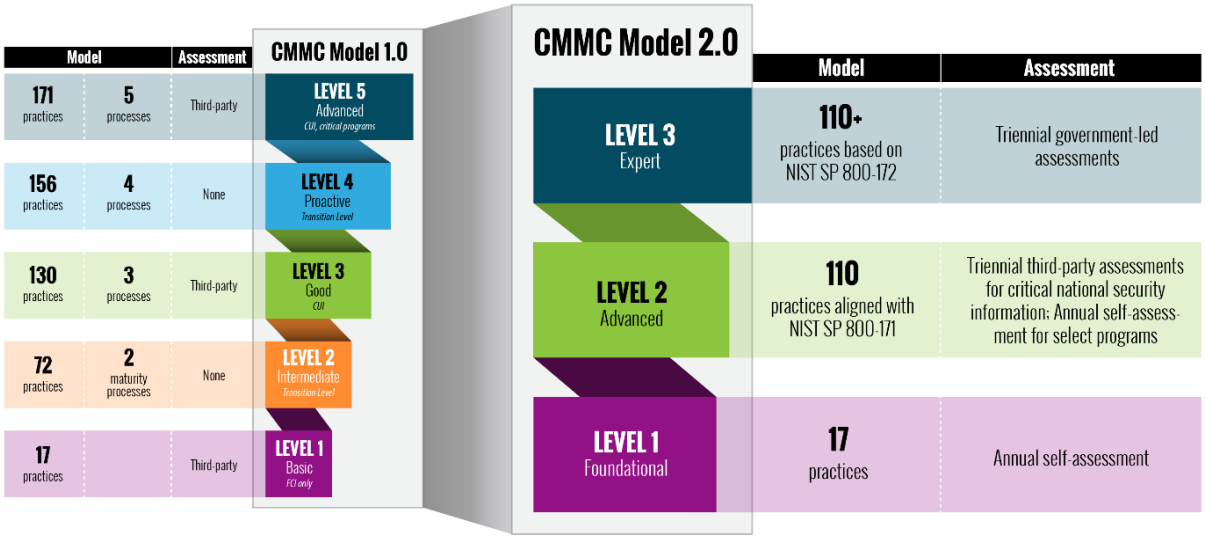
It is expected that only a small number of contracts involving the most sensitive or classified information will require CMMC level 3 certification.

What are the differences between CMMC 1.0 and CMMC 2.0?

The CMMC 1.0 framework had five levels of requirements and processes that organizations were required implement to ensure the security and protection of CUI related to a DOD-funded project. As stated above, CMMC 2.0 framework now only has three levels of requirements. This change was created by eliminating levels 2 and 4 of the 1.0 framework and removing CMMC-unique practices and all maturity processes from the CMMC model:

CMMC 1.0	CMMC 2.0
• Level 1: Basic Cyber Hygiene • ~~Level 2: Intermediate Cyber Hygiene~~ • Level 3: Good Cyber Hygiene • ~~Level 4: Proactive~~ • Level 5: Advanced/Progressive	• Level 1: Foundational • Level 2: Advanced • Level 3: Expert

The DOD Office of Acquisition and Sustainment (A&S), which is more heavily involved in the CMMC 2.0 implementation compared to 1.0 (that was mostly controlled by CMMC-AB), states that this change creates a more streamlined process; reduces assessment costs by allowing companies at levels 1 and 2 to conduct annual self-assessments to demonstrate compliance ultimately helping more small and medium sized businesses; and allowing more flexibility through the implementation of waivers for CMMC requirements under certain limited circumstances. Further, the CMMC 1.0 model also required that all DOD contractors undergo C3PAO assessments for CMMC compliance, but CMMC 2.0 only requires levels 2 and 3 to undergo a C3PAO assessment.



Source: https://www.acq.osd.mil/cmmc/about-us.html

Will this affect my organization?

Yes. Eventually, CMMC requirements of varying levels will appear on all DOD solicitations for contracts and grants that exceed the micro-purchase threshold of $10,000. Although a number of higher education and research associations have argued that DOD should exempt fundamental research from CMMC requirements, it is unlikely that DOD will exempt certain categories.

DOD's analysis found that the department awards on average 485,859 contracts and orders that would be affected to 39,204 unique awardees, of which 262,509 awards are made to 26,468 small entities. DOD also acknowledges that R&D in the physical, engineering, and life sciences fields would be among the top five industries impacted by the rule.

When will CMMC be implemented?

The changes in CMMC 2.0 will be made through the rulemaking process in 1) title 32 of the Code of Federal Regulations (CFR), to establish the CMMC 2.0 program; and, 2) title 48 CFR, to implement any needed changes to the CMMC program content in 48 CFR. Both rules are currently open for public comment and program requirements will not be mandatory until the title 32 CFR and title 48 CFR rulemaking processes are complete.

Previously the DOD announced that they would gradually integrate the requirements by distributing pilot programs starting with 15-20 in year one. Those CMMC piloting efforts have been suspended until CMMC 2.0 changes become effective. The timeline of implementation remains the same, with the DOD broadly adopting CMMC requirements across all contracts, solicitations, and grants on October 1, 2025.

What do I need to do?

Lewis-Burke recommends that staff who handle cyber or information security, as well as contracting officers, are aware of and understand these new requirements. Lewis-Burke will continue to report on new developments and updates on the CMMC.

Additional Information:

- Information on the CMMC framework can be found here.
- DOD's September 29 interim rule implementing the CMMC, "Assessing Contractor Implementation of Cybersecurity Requirements," can be found here.
- November 2021 CMMC 2.0 Updates and Way Forward Interim Rule can be found here.
- DOD launched a website to help explain CUI policy and training, and to provide a registration of CUI categories here.