protiviti®
Global Business Consulting

U.S. Department of Defense Updates Cybersecurity Maturity Model Certification Requirements: CMMC 2.0

November 10, 2021

On November 4, 2021, the U.S. Department of Defense (DoD or Department) published a proposed update to its Cybersecurity Maturity Model Certification (CMMC) and defined a path forward that has Defense Industrial Base (DIB) contractors eager to understand impacts to their business and anticipated next steps in the evolution of the CMMC program.

In addition to simplifying and consolidating the original CMMC program, CMMC 2.0 is intended to provide several improvements, including:

- Reducing assessment costs for all companies at Level 1 (Foundational) and a subset of companies at Level 2 (Advanced).
- More clearly aligning with widely accepted National Institute of Standards and Technology (NIST) cybersecurity standards and removing non-NIST controls that were in CMMC 1.0.
- Adding flexibility and speed by allowing waivers to CMMC requirements under certain limited circumstances.

Overview of the CMMC program

As detailed on the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) website, the CMMC program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

The framework has three key features:

- **Tiered model**: CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.
- **Assessment requirement**: CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- **Implementation through contracts**: Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

What is the Defense Industrial Base?

The Defense Industrial Base supports products and services essential to meeting U.S. military requirements, including research and development, design, production, delivery and maintenance of military weapon systems. More than 300,000 companies are in the DIB supply chain performing under contract with the DoD.

Overview of CMMC 2.0

CMMC 2.0 builds on the fundaments of CMMC 1.0 (introduced in January 2020) while refining the original program requirements. Under CMMC 2.0, the certification program is consolidated from five compliance levels into three:

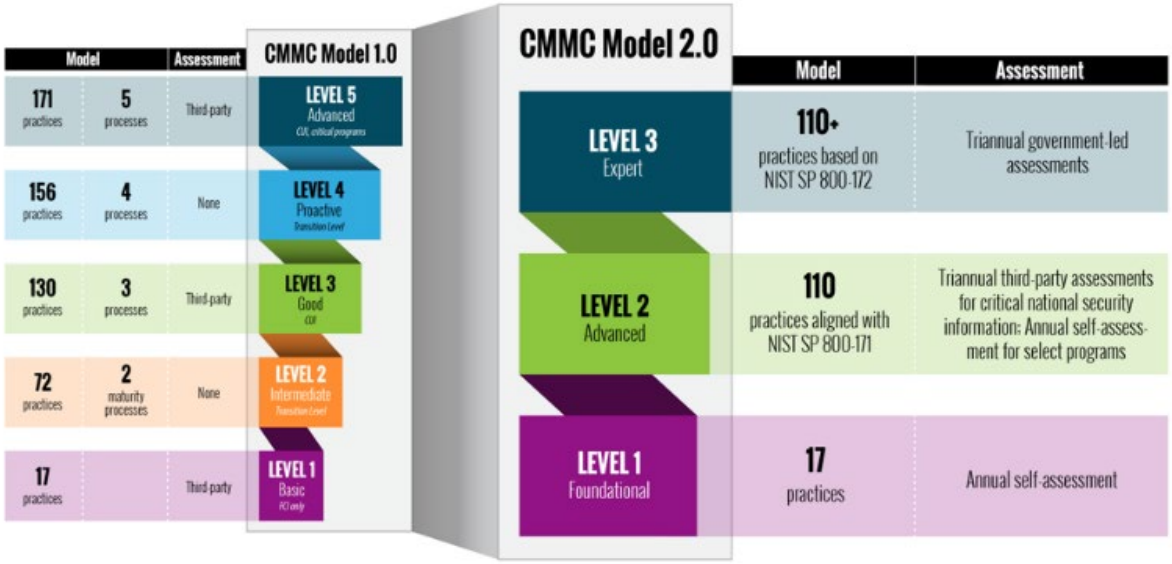
Level 1 -- Federal Contract Information (FCI) only

Level 1 (Foundational) is for systems that contain only Federal Contract Information (FCI) and have successfully implemented the 17 controls defined in the FAR 52.204-21. Contractors in Level 1 will be able to self-certify their compliance annually.

Levels 2 and 3 -- Controlled Unclassified Information (CUI)

Level 2 (Advanced) will have 110 practices that align with NIST Special Publication 800-171 with a focus on Controlled Unclassified Information (CUI). Contractors will need to undergo an assessment every three years from a certified CMMC Third-Party Assessor Organization accredited by the CMMC Accreditation Body.

Level 3 (Expert) will have more than 110 practices based on NIST SP 800-172, a supplement to NIST SP 800-171 that focuses on advanced persistent threats. Level 3 contractors will need to obtain a third-party certification from the DoD assessment teams every three years.



The Evolution to CMMC 2.0

The Road Ahead

According to the OUSD(A&S), the Department intends to pursue rulemaking for CMMC 2.0 both in Part 32 of the Code of Federal Regulations (CFR) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR. Both rules will have a public comment period. Stakeholder input is critical to meeting the objectives of the CMMC program, and the Department will actively seek opportunities to engage stakeholders as it drives towards full implementation of CMMC 2.0.

The Department intends to suspend the current CMMC Piloting efforts while the rulemaking efforts are ongoing and will not approve inclusion of a CMMC requirement in any contract before completion of the CMMC 2.0 rulemaking process. Contractors are encouraged to continue to enhance their cybersecurity posture during the interim period while the rulemaking is underway. The DoD is exploring opportunities to provide incentives for contractors who voluntarily obtain a CMMC certification in the interim period. Additional information will be provided by the Department as it becomes available.

Timeline for compliance with CMMC 2.0

CMMC 2.0 will not become a contractual requirement until the rulemaking process is completed, which is expected to take 9 to 24 months. Until then, the DoD is defaulting to the DFARS Interim Rule issued in September 2020, which is currently in effect. Only a few select pilot contracts are required to meet CMMC compliance during this period, as approved by the OUSD(A&S).

In the interim, organizations should focus on implementing all security controls cataloged in the current regulations NIST SP 800-171 framework (110 in total), as mandated in the DFARS 252.204-7012 and FAR 52.204-21. Once the rulemaking process is complete and CMMC 2.0 has been codified, the Department will require companies to adhere to the revised framework.

Next steps to prepare for CMMC 2.0

Organizations that have already developed their system security plan (SSP) and Plan of Actions & Milestones (POA&M) and have computed and submitted their Supplier Performance Risk System (SPRS) score, are well positioned to navigate the shift to CMMC 2.0.

Organizations that have yet to complete these requirements can take advantage of the rulemaking period to document and improve their cybersecurity posture through the following actions:

- Define and document a technical boundary where CUI is received, processed and stored.
- Define how CUI information will be shared with upstream partners and government sponsors.
- Document the organization's security posture to be compliant with the current DFARS rules.
- Document control implementations in a corresponding SSP.
- Identify gaps and remediation plans in a POA&M.
- Generate and upload a DOD Assessment Score into the SPRS.

- Ensure the Cybersecurity Incident Response Plan (CIRP) is updated and tested annually.
- Continue to improve the organization's security posture and SPRS score until CMMC 2.0 goes into effect.

Organizations that do not complete these actions risk noncompliance and potentially losing the ability to secure U.S. government contracts.

This is the next step of what is expected to be many as part of the current administration's focus on cybersecurity and drive to increase the cybersecurity posture of the United States. We anticipate increased regulation and penalties in the future. All organizations should take necessary steps to document and strengthen their cybersecurity programs.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2021 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

How Protiviti can help

Protiviti and its wholly owned subsidiary Protiviti Government Services are positioned to advise organizations on compliance issues, including best practices for commercial organizations to implement cybersecurity initiatives such as CMMC. Protiviti Government Services is a CMMC-AB Registered Provider Organization (RPO).

protiviti®