

Getting Started with CMMC Compliance & Key Updates in “CMMC 2.0”

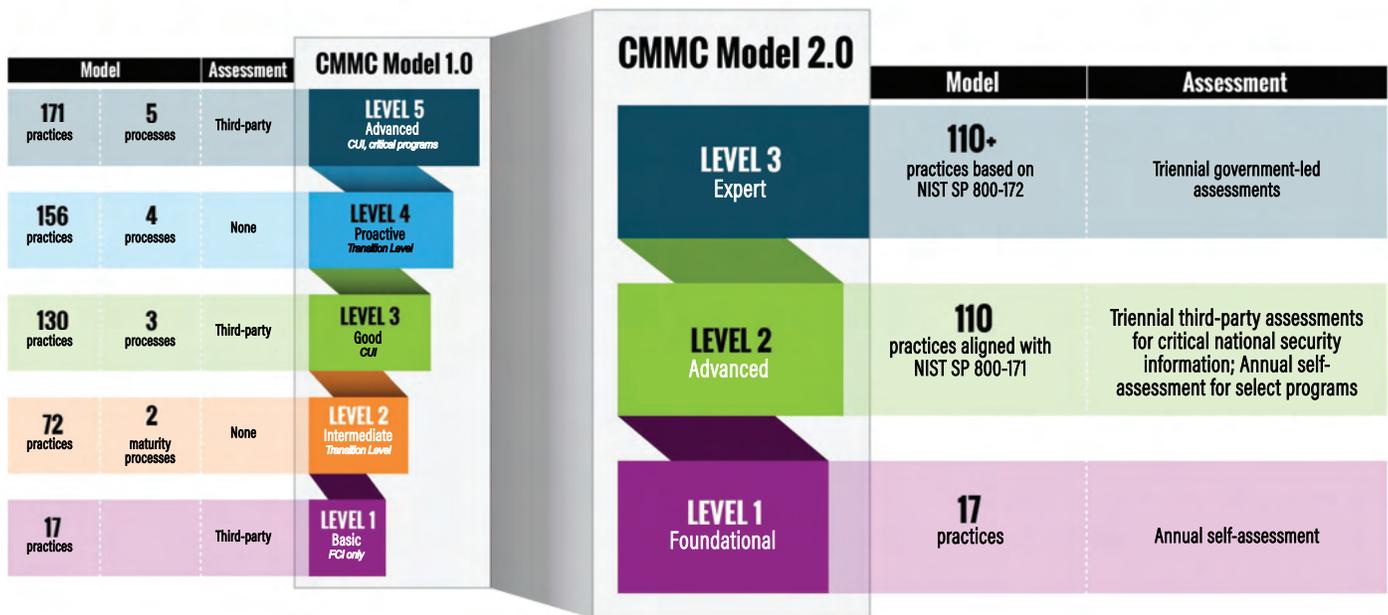
Beginning now, more than 300,000 companies and subcontractors that conduct business with the U.S. Department of Defense (DoD) will have to certify—and potentially overhaul—their cybersecurity controls and policies to comply with the Cybersecurity Maturity Model Certification (CMMC) or face a tremendous impact to their bottom line. In a recent **Security Management** article, DoD contractor and cybersecurity expert **SSE** outlined these challenges and how companies should plan to meet them.

Whether your organization works directly with the federal government or is a subcontractor, the requirements of the DFARS Interim Final Rule and the newly announced CMMC 2.0 guidelines apply. Failure to comply with these requirements could prevent future contracts, task orders or delivery orders awards. But, worse than that, failure to comply could bring litigation under the False Claims Act. Certainly, it’s a position in which no company wants to find itself.

Key Updates in CMMC 2.0

The DoD announced in late 2021 that CMMC version 1.0 will be replaced with a streamlined program called CMMC 2.0. The previous model that had 5 levels has been simplified to 3 levels:

- Level 1 “Foundational” remains unchanged
- Level 2 “Advanced” is what Level 3 was formerly, but has been simplified to align with the 110 practices of NIST 800-171
- Level 3 “Expert” is what Level 5 was formerly, with additional specifics on the number of practices to be defined by the DoD



Assessment Requirement

Depending on your compliance level, an annual self-assessment with affirmation from senior company leadership or a triennial third-party assessment is required. This differs from the previous CMMC version 1.0 requirements of triennial assessments across all levels but adds additional accountability with annual assessments and affirmation required from senior company leadership.

Limited Use of POAMs (Plans of Action and Milestones)

Under CMMC 1.0 organizations either met all practices or they didn’t, and POAMs were not allowed. CMMC 2.0 will allow “limited use” of POAMs, however, they will be strictly time-bound and limited in scope. Potentially up to 180 days was offered as the timeline allowed for remediation, and the DoD stated that POAMs would not be allowed for the highest weighted requirements. It is anticipated that nearly half of Level 2 requirements would not be allowed to have POAM items. Lastly, the DoD stated that they would also be establishing a minimum assessment score required to support certification with POAMs.

Expedited Timeline

Right Now

- NIST 800-171 related provisions call for:
 - Submission of MANDATORY Self-Scoring Required (Weighted 110 Point Scale)
 - Tracked in DoD Supplier Performance Risk System (SPRS)
 - Submission of SSPs and POAMs May Be Required

CMMC Timeline

- January 2020 CMMC 1.0 Released
- November 30, 2020 DFARS Rule Change...Interim Final Rule Effective
- November 2021 CMMC 2.0 Announced
- September 2022 Earliest CMMC 2.0 Becomes Law Following Rulemaking Process
- December 2023 Latest CMMC 2.0 Becomes Law Following Rulemaking Process

Between September 2022 & December 2023 all DoD contractors will need to meet CMMC requirements

How To Get Started

STEP 1

PLAN | Readiness Assessment - Starting with our Readiness Assessment to identify any problem areas will save time and money in the long run. A few questions to consider to ensure overall preparedness for compliance include: Will you need consultant and vendor support to get your arms around the requirements? How much budget and time will be necessary to remediate any unmet requirements?

STEP 2

PREPARE | Determine CMMC Maturity Level and Assess Gaps - CMMC compliance has three maturity levels, based on the nature of an organization's work with the DoD. Understanding which level your organization is subject to is a critical first step in the assessment process. Evaluating and documenting your current security systems and processes for gaps in the requirements, considering your current IT policies and procedures—as well as your hardware and software, is a critical step in developing a roadmap to compliance. If initial compliance efforts are incomplete or fail to meet requirements, remediation could extend the process further.

STEP 3

PROTECT | Remediation of Gaps - Once a gap assessment has been completed and a strategy has been developed, you can begin implementing necessary changes. While working through the remediation stage, you may also consider Cybersecurity-as-a-Service solutions that help automate security processes for ongoing CMMC compliance. Experienced partners can provide policy templates for mapping these solutions to a vetted tech stack of IT tools. Be sure to look for partners who have experience with DoD requirements and are verified by the CMMC Accreditation Body (CMMC-AB).

STEP 4

PERFORM | Continuous Monitoring - Compliance is not a one-time effort or snapshot. It requires around-the-clock management of IT tools, policies and procedures. To ensure ongoing compliance, a plan should be put into place for continuous monitoring and remediation of issues, along with ongoing auditing and collection of evidence to support your compliant posture. Federal contractors should be prepared to annually conduct internal self-assessments.

SSE Can Help You Prepare Your Business

At SSE, we know these evolving requirements can feel overwhelming. As a Registered Provider Organization (RPO) with the CMMC-AB, we are up to speed on the latest changes. Our team has the vetted IT tools, policy templates and assessment services mapped to NIST 800-171 and CMMC requirements to assist businesses on the road to compliance.

Let us demonstrate how we can help in preparing your business. Schedule your complimentary CMMC Readiness Assessment to get started.

[SCHEDULE TODAY!](#)

For further information or for technical assistance from SSE, please contact - Robert Duffy - Vice President of Business Development and Client Engagement
robert.duffy@sseinc.com | (314) 439-4769 | www.sseinc.com



SSE Certified as a Registered Provider Organization (RPO) by the CMMC Accreditation Body (CMMC-AB)

