CMMC Compliance MADE Easy!

(314) 439-4769

NIST 800-171 and CMMC Compliance

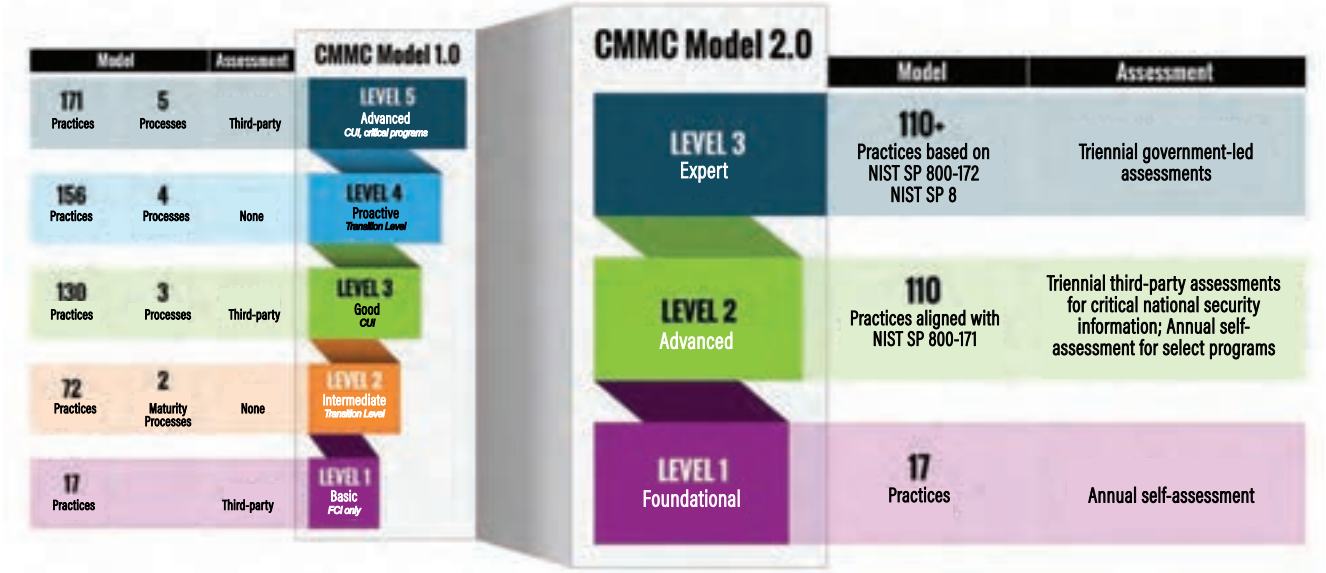
Since becoming law in 2017, NIST 800-171 has governed the protection of Controlled Unclassified Information (CUI) by DoD contractors and subcontractors. Companies must adhere to the specific 110 controls of NIST 800-171 in order to be eligible for and complete government projects that involve CUI. While companies may have been able to "self-attest" to NIST 800-171 requirements in the past, the DoD has strengthened its review and enforcement.

With the implementation of the DFARS Interim Final Rule in 2020, companies are now required to submit a scored self-assessment into the DoD's Supplier Performance Risk System (SPRS) based on their compliance with the 110 requirements of NIST 800-171. And, later this year as currently outlined by the DOD, Defense contractors and subcontractors will have to certify—and potentially overhaul—their cybersecurity controls and policies to comply with Cybersecurity Maturity Model Certification (CMMC). Companies that fail to abide by the cybersecurity standards required by their contracts may face hefty penalties. Penalty fines, which can be as much as the entire contract value, combined with the potential loss of government contracts, could create substantial risks to businesses' revenue streams.

Key Updates in CMMC

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.

Compliance Planning

The DoD has recently stated they do NOT want contractors to wait to satisfy CMMC requirements, especially if already required to meet NIST 800-171 standards in their contracts. In a June 2022 memo, the DoD reminded acquisition officials of NIST 800-171 requirements in place NOW and potential remedies for non-compliance if companies do not make progress on their submitted plan of action and milestones (POAMs). This includes auditing a company's NIST 800-171 assessment.

Additional information on back

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, But All Must Have This Documentation

CMMC Timeline

• January 2020	CMMC 1.0 Released
• November 2020	DFARS Rule Change...Interim Final Rule Effective
• November 2021	CMMC 2.0 Announced
• July 2023	CMMC Headed to the Office of Information and Regulatory Affairs (OIRA) for Review
• September 2023	Proposed Rule Expected to be Issued with a 60-Day Public Comment Period

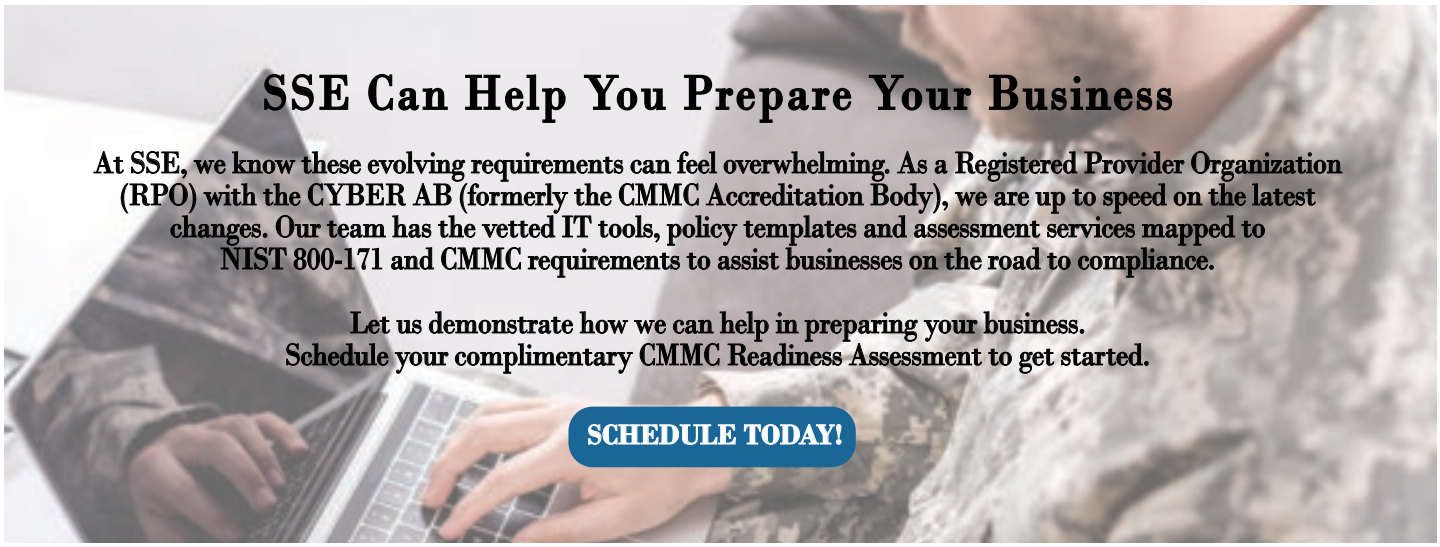
How To Get Started

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 accredited by the CYBER AB (formerly the CMMC Accreditation Body).

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.



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

nqa ISO 9001 QUALITY MANAGEMENT

SSE is accredited by the CYBER AB (formerly the CMMC Accreditation Body) as a Registered Provider Organization (RPO)

certified WBENC WOMEN'S BUSINESS ENTERPRISE