CMMC Compliance MADE Easy!

www.sseinc.com

NIST 800-171 and CMMC Compliance

Since 2017, NIST 800-171 has governed the protection of Controlled Unclassified Information (CUI) by the Department of Defense (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.

The DoD has released a Proposed Rule to officially implement its Cybersecurity Maturity Model Certification (CMMC) program. Published in the Federal Register on 12/26/23, the 234 page Title 32 Proposed Rule and supplementary information provides the requirements for DoD contractors, subcontractors and assessment organizations and moves towards implementation of a phased rollout plan starting in 2024.

CMMC Rule and Key Updates for 2024

The requirements have not changed and are not being delayed.

- CMMC Levels 1, 2 and 3 remain from the tiered CMMC 2.0 model.
- CMMC Level 2 will mirror the 110 security controls in NIST SP 800-171 Rev2, which have been requirements since 2017.
- Companies that handle CUI will need to achieve CMMC Level 2 to be able to continue supporting DoD contracts.
- The Rule details a phased rollout starting in 2024 and ending in 2026.

Assessments will be required at all CMMC levels, with annual affirmations from company leadership.

LEVEL 1 Foundational — Approximately 140K companies will require an annual self-assessment with affirmation from company leadership.

LEVEL 2 Advanced — Approximately 80K companies will require a third-party certification assessment with annual affirmation from company leadership. *Note: Only a small portion of Level 2 companies (approximately 4K may be able to self-assess.*

LEVEL 3 Expert — Approximately 1500 companies will require a DoD sanctioned certification assessment with annual affirmation from company leadership.

While NIST 800-171 currently allows Plans of Action and Milestones (POAMs) for unmet requirements, CMMC will ONLY permit the use of POAMs in the following circumstances:

- Companies must have a minimum NIST 800-171 assessment score of 88 (80%).
- POAMs will only be allowed for the 1-point controls.
- POAMs must be closed within 180 days, and a re-assessment must occur upon completion.

Estimated Cost Impact

- DoD continued not to include the cost of implementing the required controls in their impact analysis, as it maintains all contractors should already have had unchanged NIST 800-171 Rev2 controls in place as required since 2017.
- The only costs that the DoD utilized in their impact analysis were the costs of certification assessments.
- Based on the DoD's estimates, it should be expected that costs may exceed $100K for each Level 2 certification assessment.

Outside Services

- Cloud Service Providers (CSPs) and Managed Services Providers (MSPs), should be reviewed to ensure they satisfy all requirements of the CMMC Rule and DFARS 252.204-7012.
- MSPs that handle CUI or Security Protection Data must meet the same CMMC Level requirements that apply to contractors.

Increased Risk for Company Leadership

- DoD will be looking for companies even at Level 1 to demonstrate rigor in their self assessment. Level 1 and Level 2 companies need a "formal" process to self-assess annually.
- Annual affirmation/submission to Supplier Performance Risk System (SPRS) without supporting documentation risks False Claims Act liability.
- Some existing POAMs may no longer be allowed.
- Insufficient or incomplete cloud or IT/cybersecurity support services could result in failed audits and added expense.

Anticipated Timeline

- 60 day public comment period (12/26/23 - 2/26/24)...followed by adjudication of public comments/interim publication period
- A Title 48 Rule, which would provide for DoD's implementation of the Rule by contracts, is expected in March 2024
- Finalization of the Title 32 CMMC Rule and CMMC appearance in DoD contracts is expected between April 2024 and early 2025
- Phased rollout with all DoD contracts are "intended" to include CMMC assessments by October 1, 2026

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 - 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.

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 meet 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. 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 and affirm their compliance status to the DoD.

For further information, 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)