



CMMC 2.0

EVERYTHING YOU NEED TO KNOW

The Department of Defense (DoD) has initiated the formal evaluation process for the Cybersecurity Maturity Model Certification (CMMC) regulation. As this significant step unfolds, the Defense Industrial Base (DIB) and Managed Services Providers (MSPs) who work with them must understand the potential scenarios and timelines. The CMMC mandate is projected to be included in government contracts as early as Q1 of 2025, and the certification timeframe for businesses can be lengthy. A typical timeframe for understanding, developing, and implementing full CMMC 2.0 compliance is between 12 and 18 months, assuming the skills and personnel are available to complete the objectives.

REGULATORY SCENARIOS

The following scenarios and timelines should be considered in preparing for compliance and certification for the Defense Industrial Base (DIB) to ensure certification is complete by the anticipated contract inclusion date.

Scenario 1: Proposed Rule
Submission to OIRA: The Department of Defense (DoD) has officially submitted the CMMC rule for regulatory review to the Office of Information and Regulatory Affairs (OIRA).
Review and Publication: OIRA's 90-day review, which started on July 25, has concluded. The OMB Director has granted a 30-day extension. We anticipate the primary CMMC proposed rule to be published in early November , initiating the public comment phase. The OIRA extension is set to expire on November 21, 2023.
Public Comment Period: A standard 60-day public comment period will follow, ending in January 2024.
Finalization: The CMMC rule will be published as a "proposed rule," which means it will only become effective after the agency responds to public comments in a final rule. <i>Based on historical data, the average time for DoD proposed rules to be published as final rules is 333 business days.</i> This means the CMMC final rule is expected between February and April 2025.
Phased Roll-Out: The DoD plans a 3-year phased roll-out for CMMC contract clauses. Assuming the final rule is published in Q1 2025, <u>all</u> relevant DoD contracts will contain CMMC by 2028.
Scenario 2: Interim Final Rule
Immediate Effectiveness: <i>If the CMMC rule is published as an "interim final rule", it will be effective before the agency responds to public comments.</i> This means the rule would be in effect and appear in contracts in Q1 2025.
Rarity of Interim Final Rules: Such rules are rare and bypass the usual democratic process of "notice and comment" rulemaking. They are typically granted in urgent situations, like the need to enhance national security.

PLAN OF ACTION AND MILESTONES (POAM)

Like current DFARS and NIST requirements, interim CMMC status vs 100% compliance can be presented.

- ✓ These interim reports can be handled in the traditional manner by presenting a Plan of Action and Milestones (POAM) that have a less than 180-day completion date for allowed baseline gaps.
- ✓ Unallowed gaps will have a “No POAM” designation and must be implemented.
- ✓ If you have any doubts, work with a highly skilled 3rd party with expertise in these standards and a track record of enabling comprehensive, successful standards-based cyber programs.
- ✓ The information presented by the suppliers in POAMs or claiming 100% compliance will be evaluated.
- ✓ It can and will likely trigger audits if specific high-level cyber controls are unmet or the 100% compliance score creates suspicion of a false claim.
- ✓ Be careful to present accurate and validated information.

WHY ACT NOW ON CMMC 2.0

Current contracts require compliance with DFARS clause 252.204.7012 and NIST 800-171 today. The False Claims Act applies to all cyber compliance representations. If an organization is not compliant, it could be subject to civil penalties and criminal charges. CMMC 2.0 clearly aligns with DFARS and NIST, so it is the best way to protect your organization’s sensitive data.

The deadline for the final CMMC rule is slated for Q1 of 2025, and at that time, the CMMC rule will appear in some contracts with the remainder phased in over 3 years—with all relevant DoD Defense Industrial Base (DIB) contracts containing CMMC by 2028.

Since it will take an average company in the DoD supply chain 12-18 months to become prepared for assessment, the time to start the process is now if an organization is planning to hold government contracts in 2024/2025. There will also be flow-down requirements that need to be considered, which will add to the complexity.

The time to act is NOW.

