OPSPro
Enabling Your Business

CMMC 2.0 Rule is Final, Are You Prepared?

What is CMMC?

The U.S. Department of Defense (DoD) is implementing the Cybersecurity Maturity Model Certification (CMMC) to verify the cybersecurity of its supply chain. The certification encompasses three maturity levels with progressively more demanding requirements on processes and practices.

Who needs to be certified?

CMMC will impact all organizations that provide services to the DoD. The CMMC rulemaking has been completed, and CMMC will be a DoD contractual requirement and a condition for award.

Why does your business need to meet CMMC requirements?

Part of the DoD's focus on the security and resiliency of the Defense Industrial Base (DIB) sector is working with industry to enhance the protection of sensitive information and intellectual property within the supply chain.

CMMC requirements are complex, though meeting them doesn't have to be. You have **OPSPro** to assist!

As a technology partner with a specialty in Cybersecurity, OPSPro helps businesses like yours deploy security solutions that are fully integrated and helps provide end-to-end security coverage and that means we can help you put solutions in place that are already engineered to prepare your organization for CMMC.

- CMMC Assessments start in Q1 of 2025
- CMMC contract rollout expected Q3 of 2025
- Subcontractors could be required to be CMMC compliant before prime contractors issue agreements
- DoD may require Level 2 C3PAO (Certified Third-Party Assessor Organization) assessment for specific solicitations and contracts

CMMC builds upon the NIST 800-171 framework, to include controls for risk management & mitigation, incident reporting, auditing capabilities, cybersecurity and physical safeguards, and maintenance of a complete inventory of all company assets. OPSPro has a proven implementation strategy that can be customized for your specific organizational requirements.

Preliminary Assessment	Determine scope of implementation and required CMMC compliance level
Implementation Design	Customize system design and timeline specific to each organization and contract requirements
Implement / Migrate	Implement required security controls Move staff and systems to new infrastructure
Documentation	Finalize documentation to meet CMMC standards Stakeholder and staff training
Assessment	Pre-Assessment, Self Assessment, or C3PAO Assessment as required by contract

OPSPro
Enabling Your Business

Partner With us to Get Ready to Comply with CMMC in 2025

Navigating the requirements of NIST 800-171 & CMMC compliance demands more than just a tactical approach; it requires a strategic partnership with a security provider that understands the full scope and scale of cybersecurity challenges today. We would be happy to share with you a deeper overview of how we can help you meet CMMC requirements.

Contact Us Today