DoD SMALL BUSINESS BULLETIN

CMMC 2.0 is Here

Key Dates, Rules, and Resources

What's New: CMMC is Now Official

On September 10, 2025, the Department of Defense (DoD) published its final Cybersecurity Maturity Model Certification (CMMC) rule in the Federal Register, which takes effect on November 10, 2025 – officially launching a three-year rollout of cybersecurity requirements across DoD contracts.

The rule that makes these new contract requirements official is called the Cybersecurity Maturity Model Certification Program and is implemented by the Defense Federal Acquisition Regulation Supplement (DFARS), which is part of Title 48 of the Code of Federal Regulations (CFR). This is different from the separate 32 CFR rule, so don't mix them up. The two important DFARS clauses that will now appear in DoD contracts are 252.204-7021 and 252.204-7025 .

The DoD is rolling the new CMMC requirements out over three years, but by the fourth year every contractor will have to be fully compliant. At the same time, the CMMC program itself is governed by 32 CFR Part 170, which was finished in late 2024 and works alongside the 48 CFR acquisition rules.

This announcement delivers the news businesses have been waiting for, and it is now official. Beginning November 10, contracting officers will include the new CMMC requirements in new solicitations and contracts, making cybersecurity a formal part of doing business with DoD and strengthening national security through stronger cyber hygiene. In the meantime, underlying cybersecurity responsibilities remain in effect and continue to apply.

Whether you are new to DoD contracting or simply need a refresher on this issue, we have you covered.

WHAT IS CMMC AND WHY DOES IT MATTER?

The DoD introduced Cybersecurity Maturity Model Certification (CMMC) in 2020 to ensure companies protect sensitive information when working on government contracts. The program requires contractors handling Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) implement adequate cybersecurity practices to protect the defense industrial base.

Prior to CMMC, DoD contractors were required to self-attest compliance with National Institute of Standards of Technology (NIST) Special Publication 800-171 – a set of cybersecurity requirements issued by NIST, a federal agency that sets technical standards to help improve innovation, security, and quality across industries.

CMMC originally introduced a more robust five-level security framework that employed third-party assessments to verify cybersecurity maturity. However, after industry and stakeholder feedback, the DoD simplified the model to three levels in November 2021, aligning it more closely with NIST SP 800-171 to ease compliance. The resulting CMMC 2.0 is more flexible, particularly for small and medium-sized businesses.

What Happens Starting November 10: The 3-Year Rollout

On September 10, 2025, the DoD moved to the implementation stage by publishing the final Defense Federal Acquisition Regulation Supplement (DFARS) rule that formally integrates CMMC 2.0 into defense contracts. DFARS is important to DoD contractors because it supplements the federal government's primary purchasing regulations. The new DFARS 252.204-7021 clause inserts CMMC requirements directly into contracts, making cybersecurity an essential part of doing business with the Department.

TIMELINE

- Phase 1 begins November 10, 2025
- Contracting officers will include CMMC Level 1 and 2 in new contracts
- Companies must self-assess and submit scores in the Supplier Performance Risk System (SPRS) system
- CMMC will eventually be mandatory after the 3-year phase-in

This milestone marks the official transition from planning to execution. It signals to all defense contractors, especially small and medium-sized businesses, that CMMC compliance is no longer optional. As cyber threats grow in scale and sophistication, CMMC is a critical safeguard to ensure the resilience and security of the supply chain that supports our national defense.

FOR EXPERIENCED CONTRACTORS

What You Should Do Right Now

- Keep your NIST SP 800-171 implementation current
- Make sure your SPRS score is up to date
- Map out which CMMC level applies to your business
- Identify and begin closing any cybersecurity gaps

Your Free CMMC Resource Kit

1. Learn about Project Spectrum via our on-demand webinar
2. Register for a free account to:
   - Access CMMC Level 1, 2, & 3 courses
   - Access free CMMC Level 1 & 2 assessments
3. Engage with a Project Spectrum Cyber Advisor

PROJECT SPECTRUM projectspectrum.io

NEW TO CONTRACTING OR NEED HELP

Free Tools and Training with Project Spectrum

The DoD Office of Small Business Programs has resources to help small and medium-sized businesses with CMMC compliance. We initiated Project Spectrum, a comprehensive platform to provide the tools and training needed to increase cybersecurity awareness and maintain compliance with DoD contracting requirements. Project Spectrum is available to help businesses navigate CMMC compliance with free training, tools, and expert support.

HOW TO GET STARTED

Learn about Project Spectrum via our on-demand webinar

Register for a free account on projectspectrum.io Access CMMC Level 1 & 2 courses and Free CMMC Level 1 & 2 assessments

Engage with a Project Spectrum Cyber Advisor: support@projectspectrum.io

We're Here to Help

Office of Small Business Programs
U.S. Department of Defense

business.defense.gov
projectspectrum.io

PROJECT SPECTRUM

Article Shared By: