Government Contracts and Privacy & Cybersecurity Update

September 2025

CMMC 2.0 Implementation Rule

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. This "CMMC Acquisition Rule" officially begins the rollout of cybersecurity requirements across DoD contracts. Specifically, DoD will implement CMMC requirements in four phases over a three-year period, based on the certification level applicable to a DoD contract solicitation or bid.

Background

CMMC is a major DOD program built to protect the defense industrial base (DIB) from cyberattacks that compromise government-related data. The CMMC model is designed to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared with defense contractors and subcontractors during contract performance.

- **Federal Contract Information (FCI)**: As defined in section 4.1901 of the Federal Acquisition Regulation (FAR), FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, excluding information provided by the Government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments."
- **Controlled Unclassified Information (CUI)**: As outlined in 32 CFR 2002.4(h), CUI is "information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls." For more details on specific CUI categories and subcategories, see the DoD CUI Registry.
- **Verification Component:** CMMC builds on existing trust-based cybersecurity regulations in DFARS 252.204-7012 by adding a verification requirement.

Scope of Applicability

All DoD prime and subcontractors planning to bid on future contracts subject to the CMMC Acquisition Rule must obtain a CMMC certification prior to award. Some contractors accessing, processing, or storing FCI (but not CUI) will minimally require a Level 1 attestation. Each DoD contract will specify the compliance level required.

The CMMC Accreditation Body has emphasized that "[a]ll DIB members should learn the CMMC's technical requirements not only for certification but for long-term cybersecurity agility. However, DoD recognizes that many DIB members are small businesses that lack the resources of their larger, prime counterparts. As a result, the CMMC Framework incorporates cost-effective and affordable controls for small businesses to implement at the lower CMMC levels."

Timeline of Implementation

The CMMC Program's implementation date is November 10, 2025, which is 60 days after publication of the CMMC Acquisition Rule. Assessment requirements will be

introduced in four phases over three years. The phases add requirements incrementally, starting with self-assessments in Phase 1 and ending with full implementation in Phase 4. By November 10, 2028, all applicable DoD solicitations and contracts will include the full CMMC requirements**.**

This phased approach allows time to train assessors and for companies to understand and implement requirements. DoD has provided a **4-Phase Implementation Timeline**, which is included at the end of this article for easy reference.

DFARS supplements the federal government's primary purchasing regulations, so the CMMC Acquisition Rule inserts requirements directly into contracts, making cybersecurity essentially a prerequisite for doing business with DoD.

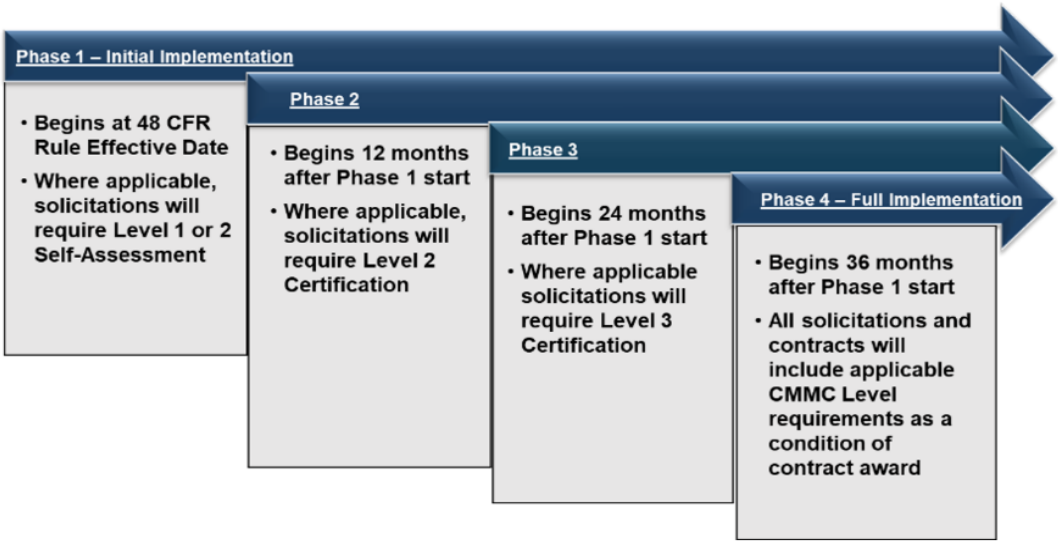
Overview of Security Assessments and CMMC Requirements

The program establishes three assessments levels, each incorporating requirements from existing regulations and guidelines:

- **Level 1: Basic Safeguarding of FCI.** Requires an annual self-assessment and affirmation of compliance with the 15 security requirements in FAR 52.204-21.
- **Level 2: Broad Protection of CUI.** Requires either a self-assessment or a C3PAO assessment every three years, as specified in the solicitation. The specific requirement is based on the type of information processed, transmitted, or stored on the contractor or subcontractor information systems. It also requires an annual affirmation and verification of compliance with the 110 security requirements in NIST SP 800-171 Revision 2.
- **Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats.** Requires an organization to achieve Final Level 2 status, undergo an assessment every three years by the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), and to provide annual affirmation of compliance with the 24 requirements in NIST SP 800-172.

Support for Small Businesses

The DoD Office of Small Business Programs offers resources to help small and mid-sized businesses with CMMC compliance. Its Project Spectrum initiative provides free training, tools, and support to strengthen cybersecurity awareness and help contractors meet DoD requirements.



FOR MORE INFORMATION

For more information, please contact:

Francis E. (Chip) Purcell, Jr.
202.263.4118
Chip.Purcell@ThompsonHine.com

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Joseph R. Berger
202.263.4193
Joseph.Berger@ThompsonHine.com