What Government Contractors Should Know About the New CMMC Rule

Client Alert
9.24.2025

The DFARS Final rule implementing the CMMC program rule has been approved and the requirements begin their two-year roll-out on November 10, 2025. This regulation is expected to reshape cybersecurity compliance for contractors with its mandatory requirements:

- **32 C.F.R. Part 170**–Establishes the **Cybersecurity Maturity Model Certification (CMMC) Program Rule**.
- **DFARS Final Rule (September 10, 2025)**–Updates the **Defense Federal Acquisition Regulation Supplement (DFARS)** to implement the Program Rule through contract clauses and policies:
  - Solicitations will include 252.204-7025 Notice of Cybersecurity Maturity Model Certification Level Requirements
  - Contracts will include updated DFARS 252.204-7021 Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements

What Is CMMC?

CMMC is a verification framework used by the U.S. government to assess a contractor's cybersecurity protections. It does not introduce new requirements but verifies that existing cybersecurity controls are properly implemented.

Key Compliance Requirements

- **Certification Is Mandatory**: Contractors must be certified and submit annual affirmations by an official to receive and maintain contracts—even those involving only Federal Contract Information (FCI) and not more sensitive Controlled Unclassified Information (CUI)

Related People

Beth S. Gotthelf
Shareholder

Joshua J. Chinsky
Shareholder

Derek Mullins
Shareholder

Claudia Rast
Shareholder

Kristina Pedersen
Associate

Related Services

Aerospace & Defense Industry Team

Cybersecurity and Privacy Specialty Team

- **Continuous Eligibility**: Compliance must be maintained throughout the life of the contract, not just at award
- **SPRS Posting**: Contractors must post their CMMC self-assessments in the Supplier Performance Risk System (SPRS) before:
  - Receiving a new award
  - Exercising an option year
  - Extending an existing contract contracting officers are prohibited from awarding or extending contracts if the contractor does not meet the required CMMC level

Subcontractor Responsibilities

Contractors must flow down applicable DFARS clauses and ensure that **all subcontractors and suppliers** annually affirm compliance with CMMC requirements, especially if they handle FCI or CUI.

Contractors should not wait to schedule their Third-Party Assessments (C3PAO)

There are only about 75–80 Certified Third-Party Assessment Organizations (C3PAOs), but over 100,000 companies may require assessments. Early action is critical, if a contractor believes they will need to be in compliance with level 2 or 3.

Cloud Storage and FedRAMP Authorization

If a contractor uses a Cloud Service Provider (CSP) to store, process, or transmit CUI:

- The CSP must meet FedRAMP (Federal Risk and Authorization Management Program) Moderate baseline requirements under DFARS 252.204-7012
- If the CSP is FedRAMP Authorized, the contractor is not responsible for the CSP's compliance
- If not authorized, the contractor must determine if the CSP meets FedRAMP Moderate equivalency

Continuous Compliance and Risks

- Contractors must:
- Maintain ongoing compliance
- Close out Plans of Action and Milestones (POA&Ms)[1] promptly
- Noncompliance risks include contract disputes and False Claims Act liability

CMMC Compliance Levels

Level 1 – FCI Only

- Annual **self-assessment**

- Results posted in SPRS
- Annual affirmation by an official

Level 2 – CUI

- Self-Assessment or Assessment by a C3PAO as determined by the specific agency
- Results posted in SPRS
- Annual affirmation by an official

Level 3 – High-Sensitivity CUI (contracts involving national security or critical defense technologies)

- Level 2 C3PAO assessment **AND**
- Level 3 assessment by Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

Contractors may be able to obtain Conditional Status

- Level 1: Only final status is permitted—no conditional awards allowed
- Level 2 & 3: Contractors may receive a conditional award for up to 180 days while closing POA&Ms

Contractors beware CMMC compliance preparation has uncovered export control violations

CMMC inspections have revealed serious issues:

- ITAR-restricted files stored in non-compliant cloud platforms (Not FedRAMP High or ensure data residency is restricted to U.S. Persons)
- Foreign nationals accessing sensitive technical documentation via Managed Service Provider teams without proper authorization
- EAR-controlled encryption technology shared on collaboration tools with global access

Timeline and Implementation

- **November 10, 2025**:
  - DoD may require Level 1 and Level 2 self-assessments for new contracts and option periods
  - Discretion to require Level 2 C3PAO certification assessments
- **November 10, 2026**:
  - Level 2 C3PAO certification assessments become mandatory
- **November 10, 2027**:
  - CMMC will be more broadly implemented but not automatically required in all contracts—contracting officers retain discretion

Please feel free to contact the authors of this Client Alert or your Butzel attorney for more information.

Beth S. Gotthelf
248.258.1303
gotthelf@butzel.com

Joshua Chinsky
313.225.7091
chinsky@butzel.com

Derek Mullins
313.983.6944
mullins@butzel.com

Claudia Rast
734.213.3431
rast@butzel.com

Kristina Pedersen
734.213.3601
pedersen@butzel.com

---

(1) POA&Ms are mandatory for CMMC certification and are used to document and monitor remediation plans for control deficiencies identified during periodic security assessments and ongoing continuous monitoring activities.