KPMG

Regulatory Alert

Regulatory Insights

September 2025

Cybersecurity: DoD Final Rule on CMMC Contract Requirements

KPMG Regulatory Insights:

- ***Preparedness:*** *Assessments permit DoD to evaluate implementation of existing cybersecurity standards; anticipate potential amendments to strengthen safeguards as needed.*
- ***Phased-In Approach:*** *Intended to provide impacted entities (DoD estimates 337,000 prime contractors and subcontractors) time to understand and implement CMMC assessment requirements.*
- ***Non-Compliance:*** *Companies should proactively evaluate cybersecurity programs against the CMMC Level 1 and Level 2 assessment guides, and complete assessments as needed; non-compliance increases risk of ineligibility for awards or possible suspension, debarment, termination, or False Claims Act violations.*
- ***Third Parties/Subcontractors:*** *Ensure subcontractors and suppliers that process, store, or transmit FCI or CUI meet the same CMMC level requirements as the prime contractor, including assessments and compliance affirmations.*

The Department of Defense (DoD)[1] finalizes a rule amending the DFARS (Defense Federal Acquisition Regulation Supplement) to formally incorporate the Cybersecurity Model Maturity Certification (CMMC) program into the DoD contracting process. The new rule requires DoD prime contractors and subcontractors to comply with the CMMC program as a condition of new contract awards involving sensitive information. The rule, commonly referred to as the 48 CFR Rule and hereinafter "Rule," becomes effective November 10, 2025. The primary features include:

1. Phased Implementation (e.g., three-year progression toward higher levels of security)
2. CMMC Program Requirements (e.g., cybersecurity standards, assessment, affirmation)

Phased Implementation

The Rule requires each new DoD solicitation and contract that requires a contractor (prime contractors and subcontractors) to process, store, or transmit information designated as FCI (federal contract information) or CUI (controlled unclassified information) to specify the necessary CMMC level (i.e., Levels 1-3) for a contractors' information system (see CMMC Program table below). The CMMC level is determined by the program office based on the sensitivity of the information and risk profile of the contract. Contractors must have a current CMMC Status at the level required by a solicitation (or higher) to be awarded a contract.

Application of the Rule will be phased-in over a three-year period:

Phase 1	Phase 2	Phase 3	Phase 4
— Begins at the Effective Date (November 10, 2025)	— Begins 12 months after Phase 1 start	— Begins 24 months after Phase 1 start	— Begins 36 months after Phase 1 start
— Where applicable, solicitations will require Level 1 or Level 2 Self-Assessment	— Where applicable, solicitations will require Level 2 Certification (by a Certified Third-Party Assessment Organization (C3PAO))	— Where applicable, solicitations will require Level 3 Certification	— All solicitations and contracts will include applicable CMMC level requirements as a condition of contract award

***NOTE**: The Rule includes a fill-in for the Contracting Officer to designate the CMMC level and level of certification required. Offerors should be aware that Contracting Officers have the option to move faster than the established phase-in schedule. Further, subcontractors may face requirements from prime contractors to meet specific CMMC levels and certifications before the government requires it.*

2. CMMC Program Requirements

The CMMC program (commonly referred to as the 32 CFR Rule was finalized in October 2024) requires contractors to meet certain cybersecurity standards based on the type and sensitivity of the information to be processed, stored, or transmitted. The program comprises a tiered model – three distinct levels, each with its own assessment and certification requirements. The Rule formally incorporates this model into the DoD contracting process.

In particular, a contractor is required to perform a self-assessment or obtain a third-party assessment (as appropriate, see table below) of its compliance with certain existing cybersecurity regulations and guidelines. As amended by the Rule, contractors must disclose their level of compliance to the DoD Supplier Performance Risk System (SPRS) and maintain continuous compliance for the life of the contract. On an annual basis, each contractor must provide affirmation, by a senior business official (the "affirming official"), that each information system the contractor uses to handle FCI or CUI is compliant, consistent with the relevant CMMC program levels.

CMMC Level	Type of Information	Plan of Action Requirements	Assessment/Certification Requirements
Level 1 Foundational (Self-Assessment)	— FCI - "Basic Safeguarding"	— None	— 15 requirements from FAR Clause 52.204-21 — Annual self-assessment — Annual compliance affirmation uploaded to SPRS
Level 2 Advanced (Self-Assessment)	— CUI – "Broad Protection"	— Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days	— 110 requirements from NIST SP 800-171A — Self-assessment conducted every 3 years — Annual compliance affirmation uploaded to SPRS
Level 2 Advanced (C3PAO)	— CUI – "Broad Protection"	— Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days	— 110 requirements from NIST SP 800-171A — C3PAO assessment every 3 years — Annual compliance affirmation uploaded to SPRS
Level 3 Expert (DIBCAC – Defense Industrial Base Cybersecurity Assessment Center (part of the Defense Contract Management Agency))	— CUI – "Higher Level Protection Again Advanced Persistent Threats"	— Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days	— Pre-requisite CMMC Status Level 2 (C3PAO) — 110 requirements from NIST SP 800-171 R2 and 24 selected requirements from NIST SP 800-172 February 2021 — DIBCAC assessment every 3 years — Annual compliance affirmation uploaded to SPRS — Annual Level 2 affirmation to also be completed

Eligibility for a contract award or extension will be contingent on having a current CMMC Status at or above the required level posted in the SPRS. Subcontractor assessment scores should be current and registered with the government. (Prime contractors will not have access to the government database and must work directly with the subcontractor to determine subcontractor compliance.)

In certain circumstances based on specific control scoring, the Rule introduces a framework that allows for a contractor that does not meet all of the necessary standards to be awarded a contract with a "conditional" status provided the contractor is actively working to close out a "plan of action and milestones" or POA&M. The POA&M is limited to CMMC Levels 2 and 3 standards and must be closed out within 180 days.

Key changes from the proposed rule include clarifications/amendments to certain definitions (e.g., "current," "CMMC Status"), clarifications to policies and procedures related to CMMC Status, and updates to the solicitation provisions and contract clauses related to identification/eligibility.

For more information, please contact Ellen Ozderman or Michael Gomez.

---

[1]*Note: The President signed Executive Order 14347, Restoring the United States Department of War, on September 5, 2025 to rename the U.S. Department of Defense to the U.S. Department of War. The Rule has been published using the name U.S Department of Defense and that has been retained in this summary.*

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com