Cooley

DoD Releases Long-Awaited Final Rule Implementing Cybersecurity Maturity Model Certification Contract Clause

September 29, 2025

On September 10, 2025, the Department of Defense (DoD) published the long-awaited final rule implementing the Cybersecurity Maturity Model Certification (CMMC) program into the Defense Federal Acquisition Regulation Supplement (DFARS). The rule takes effect on **November 10, 2025,** marking the date when contracting officers may begin inserting CMMC clauses into new solicitations and contracts.[1] The DFARS rule aligns with the CMMC program rule issued under Title 32 in December 2024, introduces a clause at **DFARS 252.204-7021**, which establishes contractors' and subcontractors' obligations, and adds a solicitation provision at **DFARS 252.204-7025**, which makes CMMC status a condition of eligibility for award.

The final rule incorporates several important updates. Each contractor system that will process, store or transmit federal contract information (FCI) or controlled unclassified information (CUI) must now have a CMMC unique identifier (UID) in the Supplier Performance Risk System (SPRS). Offerors must submit these UIDs with their proposals and update them throughout performance.[2] The rule also replaces the term "senior company official" with "affirming official," consistent with the Title 32 rule, to designate the company representative responsible for annual affirmations of compliance.[3] Award eligibility is now directly tied both to having a current CMMC status at the required level in SPRS and to maintaining a current affirmation of continuous compliance.[4] Notably, the final rule eliminates the proposed rule's requirement to report lapses in compliance with the CMMC requirements within 72 hours, but leaves the cyber incident reporting obligations in place under DFARS 252.204-7012 (DFARS 7012).[5] For subcontractor management, the rule clarifies that subcontractors must also post their assessments and affirmations in SPRS, though DoD will not share subcontractor data with prime contractors; instead, prime contractors are expected to verify subcontractor compliance directly.[6]

DFARS 252.204-7021 clause

DFARS 252.204-7021 imposes several ongoing obligations, including maintaining current CMMC status for all covered systems, flowing down requirements to subcontractors, submitting and updating CMMC UIDs, and filing annual affirmations of continuous compliance. Contractors must also close out plans of action and milestones (POA&Ms) to transition from conditional to final CMMC status.[7]

In practice, the new rule underscores several critical reminders. CMMC applies not only to CUI but also to contractor systems handling FCI, which will now require affirmations and self-assessments. Most importantly, contracting officers will be barred from awarding, extending or exercising options on contracts unless SPRS reflects the contractor's current CMMC status at the appropriate level. Prime contractors remain responsible for ensuring subcontractor compliance, even without direct access to subcontractor records in SPRS. Finally, while the rule confirms that commercial, off-the-shelf-only procurements remain excluded, most other commercial contracts will fall within scope.[8]

As a reminder, the CMMC program reflects a tiered model of cybersecurity. A CMMC Level 1 self-assessment is required to protect FCI, whereas the specific CMMC level required to protect CUI, whether it is CMMC Level 2 self-assessment, CMMC Level 2 certification assessment or CMMC Level 3 certification assessment (see below), will be determined by the DoD "based upon the sensitivity of the CUI and will be identified in the solicitation."[9]

CMMC Level 1

CMMC Level 1 will be achieved through an annual **Level 1 self-assessment**, which includes 15 requirements found in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. FAR 52.204-21 applies

to contractors who **store, process or transmit FCI**. FCI "means 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."[10]

Contractors will be required to submit their Level 1 assessment scores to the DoD's SPRS before contract award and annually thereafter.

CMMC Level 2

CMMC Level 2 will be achieved when a contractor implements the applicable security requirements in DFARS 7012 and the National Institute of Standards and Technology (NIST) Special Publication 800-171 Revision 2 practices are met. CMMC Level 2 can be achieved either through a **self-assessment** for certain contracts or through a **certification assessment** performed by a CMMC third-party assessment organization (C3PAO). CMMC Level 2 will apply broadly to contractors who **store, process or transmit CUI.** 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."[11] CUI excludes classified information.

CMMC Level 3

CMMC Level 3 will be achieved when a contractor has met the 24 selected enhanced security requirements from NIST SP 800-172, in addition to the requirements of CMMC Level 2. CMMC Level 3 assessments will be performed by the DoD. CMMC Level 3 will apply to contractors who **store, process or transmit high-value CUI.**

Phased implementation timeline

The rule also adopts a phased implementation over four years: Phase 1 begins November 10, 2025, requiring Level 1 or Level 2 self-assessments at award; Phase 2 begins November 10, 2026, requiring Level 2 C3PAO certifications at award; Phase 3 begins November 10, 2027, extending Level 2 certification to option exercises and introducing Level 3 requirements at award; and Phase 4 begins November 10, 2028, bringing full implementation across all covered contracts.[12]

Phase	Start date	Impact
Phase 1	November 10, 2025 (the date the CMMC Title 48 rule becomes effective)	Inclusion of Level 1 (self) or Level 2 (self) requirement in applicable solicitations/contracts (as a condition of award)
Phase 2	November 10, 2026 (one calendar year after Phase 1 begins)	Level 2 (C3PAO) (third-party certification assessment) requirement in applicable solicitations/contracts (as a condition of award)
Phase 3	November 10, 2027 (one calendar year after Phase 2 begins)	Level 2 (C3PAO) as a condition for exercising option periods and Level 3 Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) requirement for all applicable solicitations/contracts (as a condition of award)
Phase 4, full implementation	November 10, 2028 (one calendar year after Phase 3 begins)	Full implementation of the CMMC requirements in all applicable solicitations and contracts, including option periods

To ensure readiness with the new CMMC requirements, we recommend that clients focus on the following:

- **Review contracts and solicitations:** Identify where FCI or CUI is handled, as CMMC requirements may be added to awards with little notice after November 10. Companies should review contracts and solicitations for language or markings that signal the presence of FCI or CUI. Examples include document markings such as "CUI," "controlled" or references to export-controlled data. The inclusion of FAR 52.204-21 generally indicates that FCI is in scope, while DFARS 7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting) is a strong indicator that CUI will be involved.
- **Assess subcontractor compliance:** Revise subcontract agreements based on updates to prime contract flow-down requirements and confirm subcontractors are prepared to meet applicable CMMC levels.
- **Update corporate policies:** Ensure cybersecurity policies are current, accurate and robust enough to support compliance.
- **Refine your system security plan (SSP):** Confirm the SSP accurately reflects your current systems, scope and implementation of security controls.
- **Schedule assessments:** Arrange for required CMMC-certified assessments or complete the necessary self-assessments to maintain award eligibility.

Notes

1. 90 Fed. Reg. 43,560 (Sept. 10, 2025).
2. Id. at 43,567 – 68.
3. Id. at 43,571.
4. Id. at 43,564.

5. Id. at 43,562.
6. Id. at 43,566.
7. Id. at 43,566.
8. Id. at 43,562, 43,565.
9. 88 Fed. Reg. at 89,069.
10. 48 CFR §4.1901.
11. 32 CFR § 2002.4(h).
12. 90 Fed. Reg. 43,565 (Sept. 10, 2025).

Key Contacts

David Fletcher **Washington, DC**	**dfletcher@cooley.com** **+1 202 728 7046**
Emily Mok Reston	emok@cooley.com