SQUIRE PATTON BOGGS

The CMMC DFARS Final Rule Goes Live:

Ready or Not, Here it Comes!

US – September 2025

On September 10, 2025, the Department of Defense (DoD) issued the anticipated final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to implement the Cybersecurity Maturity Model Certification (CMMC) Program contractual requirements for defense contractors. The final rule is effective November 10, 2025.

Background

The CMMC Program requires defense prime contractors and subcontractors to (i) implement security safeguards for any contractor information systems that process, store or transmit Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), as well as (ii) maintain such safeguards throughout contract performance.

DoD first proposed the CMMC Program in December 2023, followed by a corresponding proposed DFARS rule in August 2024 (see our September 2024 alert here). In October 2024, DoD released its final rule establishing the CMMC Program (see our October 2024 alert here). In our October 2024 alert, we described the CMMC Program requirements (including the annual affirmation requirement), DoD's compliance scoring methodology and the risks for failure to comply with the CMMC program requirements. In this alert, we discuss the final rule amending the DFARS to implement the CMMC program for defense contracts.

CMMC DFARS Contractual Requirements

The DFARS final rule revises DFARS 252.204-7021 to establish contractor compliance requirements and provides for a solicitations clause at DFARS 252.204-7025, which requires the contracting officer to assign the CMMC level for each procurement, using the following language:

> (b)(1) The CMMC level required by this solicitation is: ___ [Contracting Officer insert: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)]. This CMMC level, or higher (see 32 CFR part 170), is required prior to award for each contractor information system that will process, store or transmit federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.
>
> As indicated in the clause, "prior to award" defense contractors will need to have a current CMMC certificate or self-assessment at the level specified by the contracting officer. DFARS 252.204-7025(b)(2) explicitly states that a defense contractor will not be eligible for award if the defense contractor does not have the following for each of the information systems handling FCI or CUI:
>
> 1. The current CMMC status entered in the Supplier Performance Risk System (SPRS) at the required level[1]
> 2. A current affirmation of continuous compliance in SPRS[2]

The final DFARS rule also revises DFARS Subpart 20.75 to cover the CMMC Program definitions (204.7501), policy (204.7502), procedures (204.7503) and directions for use of the solicitation provision at DFARS 252.204-7025 (204.7504).

Notable Updates and Changes from the CMMC Proposed Rule

Clarifications

- Prime contractors are required to flow down CMMC requirements to all subcontractors and suppliers that will process, store or transmit FCI or CUI on their own information systems in performance of the subcontract. There will be a requirement for a CMMC level in such subcontracts or contractual instruments. Note that the flowdown of CMMC requirements is only required when the subcontractor or supplier will process, store or transmit FCI or CUI on its own information systems. Note further that subcontracts for commercial off-the-shelf items (COTS) remain excluded from the flowdown requirement.
- For CMMC Levels 2 and 3 only, a conditional CMMC status is permitted for a period not to exceed 180 days. The final rule allows this by amending the meaning of "current", as defined in DFARS 204.7501[3]. This means, a contractor with a "current" conditional CMMC status can continue to compete for and receive contract awards as they finalize their implementation of the CMMC Level 2 or 3 requirements. The final CMMC status is granted upon closeout of any remaining Plans of Action and Milestones (POAMs). Note that, for Level 1, only final status is permitted at the time of award and no conditional status is allowed.
- The final rule established three CMMC requirements, which each have assessment requirements that include self-assessments (Levels 1 and 2), or third-party assessments conducted by a Certified Third-Party Assessment Organization (C3PAO) (Level 2) or by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) (Level 3). These assessments also flow down to subcontractors and must be posted in the SPRS.

1 DFARS 252.204-7025(b)(2)(i).

2 DFARS 252.204-7025(b)(2)(ii).

3 With regard to CMMC Status, "current" means (i) Not older than 180 days for Conditional Level 2 (Self) assessments and Conditional Level 2 (C3PAO) assessments, with (A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.16 and 170.17); and (B) A corresponding affirmation of continuous compliance by an affirming official (see 32 CFR 170.4); and (ii) Not older than 180 days for Conditional Level 3 DIBCAC assessments, with (A) No changes in compliance with the requirements at 32 CFR part 170 since the Conditional CMMC Status date (see 32 CFR 170.18); and (B) A corresponding affirmation of continuous compliance by an affirming official.

- The CMMC Unique Identifier (UID) will be issued by SPRS or Enterprise Mission Assurance Support Service (eMASS) when a CMMC assessment is made for a contractor handling FCI or CUI. Contractors are required to submit their CMMC UID to the contracting officer.

Updates

- DFARS 252.204-7021(c)(3) requires contractors to submit any changes in CMMC UIDs generated in SPRS to the contracting officer throughout the life of the contract.
- Updates what is defined as a "current" "Conditional CMMC Status", "Final CMMC Status" and "affirmation of continuous compliance," as well as further clarifies that the term "current" is related to having no changes in compliance with the requirements at 32 CFR part 170.
- The Regulatory Impact Analysis (RIA) to expand the number of estimated impacted entities to include in years four and beyond all entities in the Federal Procurement Data System awarded DoD contracts from fiscal year (FY) 2022 to FY 2024.
- The language at DFARS 252.204-7021(d)(1) no longer excludes the requirement for subcontractors to complete the affirmation of continuous compliance.
- The term "DoD unique identifier" to "CMMC unique identifier" to match the naming convention in SPRS.

Additions

- A CMMC level fill-in to the DFARS solicitation clause (DFARS 252.204-7025(b)(1))(see above).
- A definition of "FCI" based on the clause at FAR 52.204-21.
- Language to the rule to ensure the contracting officer works with the program office, or requiring activity to review the information related to the offeror's CMMC status and affirmation[4].

Removals

- The notification requirement for lapses in information security or CMMC certification in compliance with 32 CFR part 170 was removed because the reporting requirements at DFARS 252.204-7012(c) were deemed sufficient.
- The references to handling of "data" were removed and replaced with references to handling "FCI" or "CUI".
- The term "senior company official" was removed and replaced with the term "affirming official" that was codified at 32 CFR part 170.

What is the Phased Rollout to Implement CMMC (32 CFR part 170.3)?

Phase 1

Begins on effective date of the DFARS rule, which is November 10, 2025. Phase 1 will last 12 months and will therefore end in November 2026.

- **New solicitations and contracts** – Requires CMMC statuses of Level 1 (Self) or Level 2 (Self) for all applicable DoD solicitations and contracts as a condition of contract award.
- **Contracts in place prior to effective date** – DoD discretion whether to require CMMC status of Level 1 (Self) or Level 2 (Self) as a condition to exercise an option period on a contract awarded prior to the effective date. It is important for contractors to approach their contracting officers to determine if DoD will require CMMC status for upcoming options under current contracts.

Phase 2

Begins on November 10, 2026 (one year after effective date of DFARS/start of Phase 1).

- **New solicitations and contracts** – CMMC Program status of Level 2 (C3PAO) for applicable DoD solicitations and awarded contracts, but DoD has discretion to delay the requirement to an option period instead, as a condition of contract award.
- DoD also has discretion whether to include the requirement for CMMC status of Level 3 (DIBCAC) for applicable DoD solicitations and contracts.

Phase 3

Begins on November 10, 2027 (one year after the start of Phase 2).

- CMMC status of Level 2 (C3PAO) for applicable DoD solicitations and contracts as a condition of contract award, and to exercise an option period on a contract awarded after the effective date.
- CMMC Status of Level 3 (DIBCAC) for all applicable DoD solicitations and contracts as a condition of contract award.

Phase 4

Begins on November 10, 2027 (one year after start of Phase 3).

- Full implementation of the CMMC Program.
- No additional incremental requirements, DoD will include CMMC Program requirements in all applicable DoD solicitations and contracts including option periods on contracts awarded prior to the beginning of Phase 4.

4 DFARS 204.7503; DFARS 204.7504.

Compliance

On October 6, 2021, the Department of Justice (DOJ) launched its Civil Cyber-Fraud Initiative to combat emerging cyber threats to critical systems and national security of sensitive information[5]. The DOJ began to focus on government contractors that failed to follow required cybersecurity standards, which in turn has led to an increase in the prosecution of contractors under the False Claims Act (FCA) on the grounds that the contractors misrepresented their cybersecurity compliance. The new CMMC rule offers contractors an opportunity to ensure compliance with cybersecurity requirements, and through third-party assessments, it also provides contractors with potential defenses against FCA actions for misrepresentations of compliance.

Defense contractors and subcontractors that have not already been preparing to comply with CMMC are behind and need to play catch-up. Contractors need to immediately position themselves to achieve CMMC compliance and for continued success in contracting with the DoD. Check with this article's authors if you have any questions about CMMC compliance.

Contacts

Karen R. Harbaugh
Partner, Washington DC
T +1 202 457 6485
E karen.harbaugh@squirepb.com

Jeremy W. Dutra
Of Counsel, Washinton DC
T +1 202 626 6237
E jeremy.dutra@squirepb.com

Greg Jaeger
Of Counsel, Washinton DC
T +1 202 457 5296
E greg.jaeger@squirepb.com

Amjad Wakil
Associate, Washington DC
T +1 202 457 5547
E amjad.wakil@squirepb.com

Anya Bharat Ram
Associate, Washington DC
T +1 202 457 5222
E anya.bharatram@squirepb.com

5 https://www.justice.gov/archives/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.