Articles + Publications | October 1, 2025

What to Expect When the New CMMC Final Rule Hits Defense Acquisitions on November 10

WRITTEN BY

Michael E. Barnicle | Hilary S. Cairnie | Peter E. Jeydel | Bonnie Gill | Trey Smith | Bryan R. Williamson

** Tony Pappas, an associate with Troutman Pepper Locke who is not admitted to practice law in any jurisdiction, also contributed to this article.*

On September 10, the U.S. Department of Defense (DOD) posted its final rule implementing the Cybersecurity Maturity Model Certification (CMMC) program for defense acquisitions.[1] This new rule (acquisition rule) updates the Defense Federal Acquisition Regulation Supplement (DFARS) and imposes new cybersecurity requirements on defense contractors who handle (store, process, or transmit) sensitive information during contract performance.

1. Key Takeaways for Defense Contractors

- The CMMC program will begin its four-phase implementation for defense contracts and solicitations (except contracts exclusively for commercially available off-the-shelf items) on November 10.
- Defense contractors and their subcontractors will need to verify their compliance with cybersecurity standards through the CMMC program's new assessment and affirmation framework if their contracts or solicitations require them to store, process, or transmit federal contract information (FCI) or controlled unclassified information (CUI) on the contractors' information systems.
- Contractors who are not actively working toward CMMC compliance are at risk of losing future contract opportunities in the defense market.

2. The CMMC Program Under 32 C.F.R. 170

Industry stakeholders have been anticipating the acquisition rule since DOD codified the CMMC program under 32 C.F.R. Part 170, CMMC Program, on December 16, 2024 (program rule). This program is part of DOD's initiative to strengthen the defense industrial base's cybersecurity practices and protect FCI and CUI. By complying with CMMC requirements, defense contractors and vendors assure DOD that they are maintaining adequate standards for safeguarding sensitive information. The program rule accomplishes these goals by requiring contractors to assess and certify contractor information systems before contract award.

CMMC Levels and Assessment Requirements

Under the CMMC program, contractor information systems must pass a cybersecurity assessment to certify them for handling sensitive information. Each certification level (CMMC level) requires a different assessment and assessment method. DOD determines the CMMC level required for the contract and will include that information in the solicitation. There are three CMMC levels with escalating assessment requirements. Below are the general

requirements[2] by CMMC level:

- *Level 1: Basic Safeguarding of FCI.* A CMMC Level 1 is required to store, process, or transmit *FCI*. For CMMC Level 1, contractors must conduct an annual self-assessment to demonstrate compliance with all the security requirements set out in Federal Acquisition Regulation (FAR) 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*. After self-assessment, contractors must report the results by posting them on the Supplier Performance Risk System (SPRS).
- *Level 2: Protection of CUI.* A CMMC Level 2 is required to store, process, or transmit *CUI*. A CMMC Level 2 requires compliance with the 110 security requirements set out in NIST SP 800-171 Rev. 2. Contractors may satisfy Level 2 requirements either by conducting an annual self-assessment (CMMC Level 2 (Self)) or through an outside assessment conducted by a certified third-party assessment organization (C3PAO). The solicitation will specify the required assessment method. C3PAO assessments must be conducted every three years.
- *Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats.* A CMMC Level 3 is required when DOD determines the need for *higher-level protection of CUI*. To achieve CMMC Level 3, the contractor information system must first achieve a CMMC Level 2 status through a C3PAO assessment. After CMMC Level 2, the information system must undergo an additional assessment conducted by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) to ensure compliance with 24 requirements from NIST SP 800-172. DIBCAC assessments must be conducted every three years. Note that it is not clear what CUI will trigger CMMC Level 3 requirements, though it is likely related to the national security nature and sensitivity of the information.

Conditional CMMC Status and POAMs

If a contractor information system does not meet all the requirements during an assessment, a conditional CMMC status may be available in certain instances. For a conditional CMMC Level 2 or 3 status, the contractor may use a plan of action and milestones (POAM) to track remediation and cure the deficiency within 180 days. Importantly, under DFARS 204.7502, *Procedures*, a contract award can occur with a conditional CMMC level.

However, there are limitations to conditional CMMC statuses. A contractor must close out a POAM within 180 days to achieve a final CMMC status, or their conditional status will be lost. Further, POAMs are not available for CMMC Level 1. Contractors should also note that eligibility for a conditional CMMC status is based on achieving a minimum score and satisfying all “critical requirements” on the initial assessment.[3]

CMMC Unique Identifiers

Contractor information system assessments are reported in DOD’s SPRS. SPRS generates a CMMC unique identifier (UID) for each contractor CMMC assessment it receives. When a contract requires a CMMC level, an offeror must include a list of their applicable UIDs with their proposal. Contractors must also update their UID list when new codes are generated by SPRS.

Current Affirmation of Continuous Compliance

In addition to achieving a CMMC level, contractors must also “affirm” their continuing compliance with their assessment’s requirements.[4] The contractor’s affirming official (the contractor’s senior representative responsible for CMMC program compliance) must submit an affirmation electronically in SPRS upon achieving a CMMC level, and annually thereafter. In the event of a cybersecurity incident, contractors will continue to follow the reporting requirements found in DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber

Incident Reporting.

Subcontractor Flowdown

Subcontractors must also adhere to CMMC requirements when they are required to handle FCI or CUI on their subcontractor information systems. However, as the subcontractor is not in privity with the government, the prime contractor is responsible for ensuring that subcontractors comply with the CMMC program before contract award and during performance. Unfortunately, SPRS does not allow contractors to view SPRS data other than their own. Therefore, prime contractors and subcontractors must develop the mechanisms to monitor CMMC compliance throughout their supply chain to prevent issues. For more information on subcontractor compliance, *see* 32 C.F.R. 170.23, Application to Subcontractors.

3. CMMC Implementation for Defense Acquisitions

Applicability of CMMC Requirements on Acquisitions

The acquisition rule, as a DFARS rule, only applies to DOD acquisitions. Contractors engaged in contracts with non-DOD agencies should refer to the acquisition procedures of those organizations to assess their cybersecurity requirements. Further, CMMC requirements only apply to contracts where the contractor will handle FCI or CUI on contractor information systems during contract performance. Note there is an exclusion for awards solely for the acquisition of commercially available off-the-shelf (COTS) items.[5] In those limited cases, CMMC requirements do not apply.

Phased Implementation of the CMMC Program Under the DFARS

To minimize the financial impacts and disruption to the industrial base, DOD is rolling out CMMC requirements in four phases. During the first three years after the acquisition rule becomes effective (November 10), the DOD will have discretion to add CMMC requirements to certain contracts. DOD's four-phase implementation consists of the following:

- Phase 1: Begins on November 10. DOD will begin requiring CMMC Level 1 and Level 2 self-assessments for applicable contracts and solicitations.
- Phase 2: Begins one year after Phase 1. DOD will begin requiring CMMC Level 2 (C3PAO) for applicable contracts and solicitations.
- Phase 3: Begins one year after Phase 2. DOD will begin requiring CMMC Level 3 (DIBCAC) for applicable contracts and solicitations.
- Phase 4: Begins one year after Phase 3. DOD will fully implement the CMMC program on applicable contracts and solicitations.

Note that the DOD has retained discretion to delay or advance higher CMMC requirements at each phase of implementation. For more on the DOD's phased plan for CMMC implementation, see 32 C.F.R. 170.3, Applicability .

CMMC DFARS Clauses.

The acquisition rule creates two new DFARS clauses that implement the CMMC in the DOD acquisition process:

- **DFARS 252.204-7025, Notice of Cybersecurity Maturity Model Certification Level Requirements**. This is the CMMC ***solicitation provision*** that notifies offerors of a potential contract's CMMC requirements. This provision will identify the CMMC level (CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC)) required for each contractor information system that will be handling sensitive information during contract performance. This provision also states that offerors who do not have both a current CMMC level assessment *and* an affirmation of continuous compliance in SPRS will not be eligible for contract award. This clause also contains POAM closeout requirements for contractors with a conditional CMMC status. Finally, this clause requires offerors to provide a list of their UIDs (generated by SPRS) with their proposal and to update that list as new UIDs are generated.
- **DFARS 252.204-7021, Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirements**. This is the clause that will ***appear in the contract itself*** and will similarly specify the CMMC level requirement. In addition to requiring contractors to have and maintain the requisite CMMC level, this clause also requires contractors to flow down CMMC requirements to subcontractors who will handle sensitive information on subcontractor systems. This clause also restricts contractors to using information systems with the requisite CMMC level or higher for handling FCI or CUI.

4. Expected Impact and Takeaways.

The DOD estimates that CMMC program requirements will affect approximately 337,968 total contractors and subcontractors by the fourth year of the program's implementation.[6] The DOD also anticipates the greatest concentration of CMMC level requirements will occur at CMMC Level 1 (62% of contractors) and Level 2 Certificate with a C3PAO assessment (35%). While the phased implementation of the CMMC program may soften its initial impact this November, preparation of full implementation is crucial. The CMMC program is on track to become an integral part of the DFARS, and contractors must be proactive with the new cybersecurity framework to remain competitive in the defense acquisition market.

Recommendations on Next Steps

- Noncompliance with CMMC requirements will impact defense contract awards. To remain competitive, contractors should anticipate the CMMC level they will need for future contracts. Current contractors may look to past contract awards and the level of sensitive information they handled in those instances. Contractors should also develop a strategy for evaluating and remediating their information systems to pass the requisite assessment.
- Contractors must not only achieve compliance to be eligible for contract award but also *maintain* compliance through the performance of the contract. Contractors should develop internal procedures for monitoring and reporting cybersecurity information to the affirming official. This will help ensure annual SPRS affirmations are both timely and accurate.
- Depending on the nature of the contract, contractors must verify their subcontractors' CMMC compliance prior to award and during performance. Discussions about CMMC level, compliance oversight, and reporting should begin early in the contractor-subcontractor relationship. Subcontractors should also be prepared to verify their compliance during negotiations.

---

[1] For the final rule, as well as the DOD's responses to public comments, visit the *Federal Register*'s website.

[2] *See* U.S. Dep't of War Chief Info. Officer, *About CMMC*, https://dodcio.defense.gov/cmmc/About/ (last visited Sep. 16, 2025).

[3] *See* 32 C.F.R. 170.21, Plan of Action and Milestones requirements.

[4] *See* 32 C.F.R. 170.22, Affirmation.

[5] *See* Federal Acquisition Regulation 2.101, Definitions, for COTS definition.

[6] *See* Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements, 90 Fed. Reg. 43560, 43573 (Sep. 10, 2025) (to be codified in 48 C.F.R. pts. 204, 212,217, 252).

RELATED INDUSTRIES + PRACTICES

- Government Contracts