wiley

ALERT

Additional Analysis on DOD's Final Rule for the Cybersecurity Maturity Model Certification Program

September 22, 2025

WHAT: The U.S. Department of Defense (DOD) this month published the second of two final rules needed to begin phasing in the long-awaited Cybersecurity Maturity Model Certification (CMMC) Program. Below is an in-depth analysis of this final rule and compliance-related considerations, as previewed in our September 10 alert.

This final rule amends the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements for the CMMC Program. The final rule at long last triggers the phase-in plan that DOD previously outlined in the earlier final rule (which we summarized here) codifying the CMMC program requirements in Title 32 of the Code of Federal Regulations.

WHEN: DOD issued the final rule on September 10, 2025, and it will take effect on November 10, 2025. That effective date will mark the first day of the three-year phase-in effort that DOD previously prescribed. *See* 32 CFR § 170.3(e). During the first year of the phase-in plan, the following will be applicable:

- For new contracts, DOD intends to require at least a self-assessment as a condition of award. DOD retains the discretion to require a third-party certification (by a certified third-party assessment organization (C3PAO)).
- For existing contracts, DOD retains the discretion to require a self-assessment or C3PAO assessment as a condition of exercising an option.

Authors

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
lbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Practice Areas

Administrative Procedure
Cybersecurity
Emerging Technologies
Government Contractors & Grantees
Government Contracts
Privacy, Cyber & Data Governance
Strategic Competition & Supply Chain

Teaming Agreements, Strategic Alliances, and Subcontracting

WHAT DOES THIS MEAN FOR INDUSTRY: CMMC requirements will apply to contractors and subcontractors that process, store, or transmit covered information (Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)) under DOD (or DOD-funded) contracts, except for contracts exclusively for commercially available off-the-shelf (COTS) items. We expect to see requirements related to CMMC appear in solicitations starting November 10, 2025.

BACKGROUND

DOD has been laying the foundation for this final rule for over a decade. Shortly after the Government first coined the term CUI, DOD announced its earliest plans to add standard contract requirements for safeguarding this type of information in the DFARS. Since then, these requirements have taken various forms, including the safeguarding Covered Defense Information (CDI) and cyber incident reporting and flow down requirements at DFARS 252.204-7012, the subsequent certification and DOD assessment requirements in DFARS 252.204-7020, and the CMMC frameworks contractor clause in DFARS 252.204-7021.

DOD established the CMMC Program in two different parts of the Code of Federal Regulations. First, in Title 32, DOD established what it refers to as the program requirements. These regulations detail, among other things, what level of security the Government should require and what companies can do to achieve each applicable level of security. DOD first issued the proposed version of these regulations on December 26, 2023 (88 Fed. Reg. 89058) and later finalized them on October 15, 2024 (89 Fed. Reg. 83092).

Second, in Title 48, DOD established the specific requirements for contracting officers, including the contents of the standard clauses that contracting officers will be required to include in all covered contracts. DOD first issued the proposed version of these regulations on August 15, 2024 (89 Fed. Reg. 66327) (which we previously covered here). DOD's September 10 publication finalizes a version of these rules.

Overview of CMMC Program Requirements

As many in industry are aware by now, the CMMC Program requires contractors that process, store, or transmit Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) in performance of a DOD contract to adopt substantive security requirements based on the CMMC Level determined for that effort. There are three CMMC Levels with the following technical requirements:

- **Level 1:** Includes the 15 security requirements specified in FAR 52.204-21, Basic Safeguarding of Contractor Information Systems (moved to FAR 52.240-93 in the overhauled FAR). The Government will require Level 1 when the contractor's information systems will process, store, or transmit FCI but not CUI.
- **Level 2:** Includes the 110 security requirements in the National Institute of Standards & Technology (NIST) SP 800-171 Revision (Rev.) 2. These are the same requirements under DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. The Government will require at least Level 2 when it anticipates that the contractor information system will process, store, or transmit CUI.
- **Level 3:** Includes the 110 security requirements from NIST SP 800-171 Rev. 2 and 24 additional security requirements from NIST SP 800-172. The Government will require Level 3 for contracts supporting its most critical programs and technologies.

Note that the CMMC levels are keyed to requirements in NIST SP 800-171 Rev. 2, which was superseded by the publication of Rev. 3 in May 2024. Contractors are required to meet the Rev. 2 requirements for CMMC audits, but should understand Rev. 3's requirements and consider developing a crosswalk to identify the Rev. 3 equivalent for each Rev. 2 control and prepare for a future transition to Rev. 3 compliance.

In addition to implementing the relevant technical requirements, the CMMC Program requires contractors to periodically assess compliance for each covered information system.

- For CMMC Level 1 (Self) or Level 2 (Self), contractors are required to perform a self-assessment and post the score in the Supplier Performance Risk System (SPRS).
- For CMMC Level 2 (C3PAO), contractors must undergo a third-party assessment from a certified third-party assessor organization (C3PAO). A C3PAO assessment is valid for three years.
- For CMMC Level 3, contractors must obtain a C3PAO assessment confirming compliance with the Level 2 requirements and a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) certification confirming compliance with the 24 additional security requirements from NIST 800-172. Each assessment is valid for up to three years.

The CMMC Program also requires contractors to annually submit affirmation of continuous compliance through SPRS. The affirmation must be completed by an "affirming official," which is defined in the CMMC Program Rule as a senior-level representative who is responsible for ensuring the organization's compliance with the CMMC Program requirements and has the authority to affirm continuing compliance with the specified security requirements for their respective organizations. When responding to a solicitation with a CMMC requirement, offerors must identify to the contracting officer the CMMC UIDs for any information systems to be used in performance that would store, process, or transmit FCI or CUI. The contracting officer will use that information

to verify the current CMMC status for each information system. DOD estimates that contractors will have an average of five systems that will require CMMC compliance.

Timeline for Implementation. The effective date for the DFARS final rule, November 10, 2025, will be the effective date for the CMMC 2.0 Program. After this date, the clause at DFARS 252.204-7021 will be included in solicitations and in any resulting contracts.

In identifying which CMMC status, if any, to require, DOD will follow the CMMC implementation timeline set forth in the Program Rule, following a three-year phased implementation approach:

- **Phase 1:** Beginning November 10, 2025, Level 1 (Self) or Level 2 (Self) requirements will be included in applicable solicitations and contracts. DOD also has discretion to include the requirement for CMMC Level 2 (C3PAO) for applicable solicitations and contracts.
- **Phase 2:** On November 10, 2026, the requirement to conduct Level 2 (C3PAO) certifications assessments will be included in applicable solicitations and contracts. DOD also has discretion to include the requirement for CMMC Level 3 (DIBCAC) for applicable DOD solicitations and contracts.
- **Phase 3:** On November 10, 2027, Level 3 (DIBCAC) requirements will be included in all applicable solicitations and contracts.
- **Phase 4:** On November 10, 2028, the CMMC Program will be fully implemented. All CMMC requirements will be included in all applicable solicitations, contracts, and exercises of option periods.

Note, however, that DOD may choose to negotiate modifications adding CMMC requirements to contracts awarded prior to CMMC implementation and in the exercise of option periods. In the DFARS final rule, DOD declined to limit the Contracting Officer's discretion to bilaterally incorporate CMMC requirements in existing contracts based on DOD's needs and left it up to the Contracting Officer to reasonably modify existing contracts after the final rule is in effect.

Subcontractor Flow Downs. DOD clarified in the DFARS final rule that it is up to the prime contractor (or the higher-tier subcontractor) to determine what information needs to be shared with a subcontractor and, therefore, whether the subcontractor's information system would process, store, or transmit CUI or FCI during performance of the subcontract. Based on the analysis, the prime contractor will determine whether a CMMC Level requirement must be flowed down to the subcontractor. Subcontractors that process, store, or transmit FCI/CUI also must post their CMMC status and submit affirmations of continuous compliance in SPRS. DOD confirmed that prime contractors and higher-tier subcontractors will not have access to subcontractor information in SPRS, but DOD expects that subcontractors will voluntarily share any necessary information when negotiating subcontracts and teaming arrangements.

OTHER NOTABLE UPDATES

The final rule incorporates changes to address industry comments and withdraws some of the more ambiguous requirements from the proposed rule, which we covered in a previous alert.

Finalizing CMMC Conditional Status

The CMMC Program Rule envisions that some Level 2 and 3 assessments may result in a "conditional" CMMC status, pending resolution of any Plan of Action and Milestones (POA&Ms). The DFARS final rule further clarifies that a conditional CMMC status is permitted for a maximum of 180 days. A final CMMC status will be achieved upon successful closeout of all POA&Ms (including, if required, third-party assessment to achieve closeout). Neither rule, however, prescribes precisely what should happen, under existing contracts, if a contractor or subcontractor fails to close out all POA&Ms on time.

Updates to Reporting Requirements

In response to comments from industry about ambiguity in the proposed rule, DOD removed the requirement to notify the contracting officer of "lapses" in information security or "changes" in compliance. DOD determined that the reporting requirements in DFARS 252.204-7012(c) for notification of information security incidents and an annual affirmation of continuing compliance would sufficiently protect DOD information.

KEY TAKEAWAYS FOR INDUSTRY

Increased accountability. Although the technical requirements under CMMC Levels 1 and 2 are not new, the CMMC Program defines a framework to increase contractor accountability. Based on the expected number of affected contractors in the CMMC Program Rule, many contractors will be required to undergo third-party assessments of compliance before they can receive contract awards – self-assessments alone will no longer be sufficient.

Planning ahead. CMMC requires contractors to obtain CMMC UIDs for each information system that will be used to process, store, or transmit FCI and CUI. To that end, contractors should understand which information systems could be used in performance of government contracts and would process, store, or transmit FCI and CUI; where FCI and/or CUI would be stored; and how they will track compliance and prepare SPRS submissions and annual affirmations for each of those systems. This may be particularly challenging for prime contractors because the preamble indicates that DOD intends for prime contractors to include the UIDs to be used by their subcontractors.

We also expect to see increased demand for the services of C3PAOs as CMMC starts appearing in solicitations and resulting contracts. It might be difficult for contractors to ascertain which contracts will impose which CMMC Levels to ensure all relevant information systems are properly certified before the contract award. This will be an even bigger challenge as contractors seek to partner with multiple subcontractors that must also comply with CMMC requirements. Contractors should evaluate the various certification pathways and timelines for certification, and invest in vendor relationships in sufficient time to work toward achieving final CMMC status as needed for anticipated procurement opportunities. Preparations for third-party assessments should include extra time for making adjustments or corrections in response to assessment findings, which may also require subsequent assessments to evaluate corrections. Contractors should also allow time to resolve disagreements with assessors regarding compliance with the underlying security requirements, including involving counsel as necessary. In addition, contractors should review their

agreements with security service providers to ensure they allow for third-party assessments, if necessary, and prepare with security service providers in advance to facilitate successful third-party assessments.

Contractors undergoing CMMC third-party assessments should also consider what may happen if the assessment determines that information systems that currently process, store, or transmit FCI/CUI based on self-assessments do not meet all the relevant security requirements. This may include planning for addressing any POA&Ms or for review of prior assessments and any risks identified by the third-party assessment.

Prepare Your Supply Chain. Subcontractors that process, store, or transmit FCI/CUI are also subject to CMMC requirements. Prime contractors should consider their plan for flowing-down requirements, assessing subcontractor compliance, and developing alternative solutions for noncompliant subcontractors. For example, contractors might find it preferable to provide subcontractors with the information systems to process, store, and transmit FCI/CUI. This arrangement could increase the contractor's confidence in the security and readiness of the relevant systems while decreasing the added costs and time that some smaller subcontractors might not be able to afford. Of course, such a solution will also increase the cost and security and management burden on prime contractors.

Contractors have already expressed concerns related to the lack of transparency related to subcontractors and their CMMC status and scores. These requirements may also increase subcontractor costs and timelines for readiness, and prime and higher-tier subcontractors should build those issues into their proposal strategies. Contractors should consider adding contractual language in partner agreements that: (1) requires subcontractors to disclose their CMMC certification and compliance status; (2) obligates subcontractors to enter their status into SPRS in advance of the contract award; and (3) obligates subcontractors to report changes in status to the prime contractor as well as to DOD as required by the rules.

Consider Compliance Risk. Throughout the lifecycle of the contract, companies' "affirming officials" must annually affirm their continued compliance with their assessed CMMC status, in addition to existing reporting requirements, such as reporting cybersecurity incidents. It is unclear how agencies will address disruptions to continuous compliance, which could create contractual and legal risk for contractors. Also unclear is the potential liability exposure of affirming officials.

Anticipate Transition to NIST SP 800-171 Rev. 3. The current CMMC Program requires compliance with NIST SP 800-171 Revision 2, which was published in February 2020. DOD has signaled, however, that it is working toward NIST's latest version of the publication, Revision 3, which was published in 2024. We previously covered NIST's updates to Revision 3 in an alert here. As contractors are working on developing and securing information systems for CMMC, they should also keep an eye on Revision 3 and anticipate updates that may be necessary for attaining compliance with that standard if and when DOD adopts it for CMMC.

Wiley's cross-disciplinary Government Contracts, National Security, and Privacy, Cyber & Data Governance teams have extensive experience advising clients on all aspects of compliance with CMMC requirements and will continue to monitor these developments.