SEPTEMBER 15, 2025

What the Department of Defense Final Rule "Assessing Contractor Implementation of Cybersecurity Requirements" Means for Government Contractors' Information Security Systems

by Gunjan R. Talati , Jennifer L. Andrews , Katherine S. Klein

On September 10, 2025, the Department of Defense (DoD) issued a long-awaited final rule related to the implementation of the Cybersecurity Maturity Model Certification (CMMC) program. The final rule goes into effect on November 10, 2025, but we are unlikely to see CMMC requirements appear overnight in every DoD contract. Instead, there will be a three-year phased implementation. Initially, only select contracts will require CMMC; after three years, it will apply broadly to all contracts involving Federal Contract Information (FCI) or Controlled Unclassified Information (CUI)[1], except for those solely for commercially available off-the-shelf (COTS) items. Contractors will register CMMC status in the Supplier Performance Risk System (SPRS) and will be assigned a "CMMC unique identifier (UID)" for each contractor information system.

The rule mandates that contracting officers verify a contractor's CMMC status through the SPRS at the required level before awarding contracts, exercising options, or extending periods of performance. Contractors are required to post the results of self-assessments (or third-party assessments, where applicable) and provide annual affirmations of continuous compliance by an authorized affirming official in SPRS. The rule also allows for a "conditional" CMMC status at Levels 2 and 3 for up to 180 days, provided that an approved plan of action and milestones (POA&M) is in place and subsequently closed out to achieve "final" status.

New DFARS Clauses

The final rule introduces new and revised clauses that formalize CMMC requirements for DoD contracts.

DFARS 252.204-7021

The final rule updates DFARS 252.204-7021, “Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirements.” This clause now requires contractors (including applicable subcontractors) to maintain a current CMMC status at the level specified in the contract for all information systems used in the performance of the contract that process, store, or transmit FCI or CUI. The clause also requires contractors to ensure that their affirming official completes annual affirmations of continuous compliance in the SPRS.

A key new feature of the clause is its requirement for contractors to report their CMMC UID(s) for each information system used in contract performance, including a subcontractor's information system, and to update the contracting officer with any changes throughout the contract's life cycle. The clause stipulates that only information systems with the requisite CMMC level may be used for handling FCI or CUI, and it enforces a clear process for documenting and validating compliance via SPRS. Additionally, the clause outlines the conditions under which contractors may hold a “conditional” CMMC status (specifically for CMMC Levels 2 and 3) and the requirement to close out any POA&Ms to achieve final certification.

Prime contractors must insert the substance of the DFARS 252.204-7021 clause in all subcontracts or contractual instruments where the subcontractor will process, store, or transmit FCI or CUI. Subcontractors must also submit affirmations of continuous compliance in SPRS and maintain the required CMMC status prior to subcontract award.

DFARS 252.204-7025

The rule also prescribes the use of DFARS 252.204-7025, “Notice of Cybersecurity Maturity Model Certification Level Requirements,” in solicitations. This new clause informs offerors of the required CMMC level and sets forth the conditions for eligibility, namely that offerors must have a current CMMC status and affirmation in SPRS for each contractor information system, including a subcontractor's information system, that will handle FCI or CUI. DFARS 252.204-7025 requires submission of the appropriate CMMC UID(s) as part of the proposal and mandates updates if new UIDs are generated during contract performance.

How Does This Impact DFARS 252.204-7012?

As many federal contractors know, the DoD already has stringent requirements for contracts that

contain CUI. DFARS 252.204-7012 requires federal contractors and subcontractors to adequately safeguard CUI by implementing the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171, or an equivalent security protocol. NIST SP 800-171 compliance corresponds to the 110 security requirements found in CMMC Level 2.

A difference between DFARS 252.204-7012 and the clauses that will implement the CMMC final rule are that the new DFARS clauses will require contractors to register in SPRS. As in past proposed rules, the final rule states that if contractors are already compliant with DFARS 252.204-7012 but wish to perform on Level 2 contracts, they will need to either complete an annual self-assessment or obtain a triennial assessment from a Certified Third-Party Assessment Organization (C3PAO). To compete on Level 3 CMMC contracts, contractors will need to meet additional NIST SP 800-172 requirements and obtain a triennial assessment from DoD officials.

Main Takeaways for Government Contractors

- Phased Implementation and Exemptions. The CMMC requirements are being rolled out over a three-year phased implementation. Initially, only selected contracts will include CMMC requirements; after the phase-in, all applicable contracts will require compliance, except those solely for COTS items.

- CMMC Certification is Mandatory for Contract Eligibility. Contractors and their relevant subcontractors must achieve and maintain the CMMC level specified in the contract for all information systems that process, store, or transmit FCI or CUI throughout the entire contract period. CMMC compliance is a prerequisite for contract award. Offerors who do not meet the required CMMC level are ineligible for award consideration.

- Verification and Reporting Requirements. Contractors are required to post CMMC assessment results and affirmations of continuous compliance in the SPRS. Contracting officers will verify CMMC status via SPRS before awarding contracts, exercising options, or extending contract periods.

- Flowdown to Subcontractors. CMMC requirements must be flowed down to subcontractors that will process, store, or transmit FCI or CUI. Prime contractors are responsible for ensuring subcontractors' compliance at the appropriate CMMC level before sharing sensitive information or awarding subcontracts. Subcontractors must also maintain current CMMC status and submit affirmations in SPRS.

- Conditional Status and Plans of Action. For CMMC Levels 2 and 3, contractors may be awarded contracts with a "conditional" certification status for up to 180 days, provided a valid POA&M is in place and closed out to achieve final status. Level 1 requires a final status at award.

- New DFARS Clauses and Procedures. Contractors should familiarize themselves with the new DFARS 252.204-7021 and 252.204-7025 as these formalize the CMMC requirements, reporting, and flowdown obligations. Contractors are expected to integrate these clauses into their contract management and compliance programs.

- No Exemptions for Small Entities or Existing Contracts. While the rule aims to minimize burden on small businesses through phased implementation and COTS exemptions, there are no blanket waivers for small entities or existing contracts. CMMC requirements will be incorporated into new contracts and may be added to existing contracts at the contracting officer's discretion through a bilateral modification.

Footnotes

[1] Federal contract information (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, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments. *See* FAR 52.204-21. Controlled Unclassified Information (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. *See* 32 CFR 2002.4(h).