

Alert | Government Contracts



September 2025

CMMC Contract Clauses Finalized

The U.S. Department of Defense has issued a **final rule** amending the Defense Federal Acquisition Regulation Supplement (DFARS) to include contractual requirements for the Cybersecurity Maturity Model Certification (CMMC) program. The final rule supports the CMMC framework established under the National Defense Authorization Act and previous rulemakings.¹ With the final rule taking effect Nov. 10, 2025, the CMMC program, **which was finalized in October 2024** under 32 C.F.R. part 170, will be implemented in government contracts and subcontracts. Contractors should expect to see CMMC requirements included in DoD solicitations, contract modifications, and option exercises.

The **proposed contract clauses** were issued on Aug. 15, 2024. The final rule modifies the clauses in certain respects:

- **Award Policy.** DFARS 204.7502 clarifies that for CMMC Levels 2 and 3 only, contractors may receive contract awards with a conditional CMMC status for up to 180 days, as permitted under 32 C.F.R. 170.21. The final rule also specifies that a final CMMC status is granted upon successful closeout of remaining Plans of Action and Milestones (POAMs). This change will enable companies with eligible POAMs to continue to compete for and receive contract awards as they finalize their implementation of the CMMC Level 2 or 3 requirements.
- **Procedures for Contracting Officers.** DFARS 204.7503 confirms that contracts cannot be awarded to an offeror lacking current CMMC status at or above the required level for each system

¹ For a summary of the proposed rule, see [GT Alert, DoD's Proposed Rule Would Implement CMMC Contract Clauses, August 2024](#).

involved. Offerors at the prime level must provide contracting officers with applicable CMMC unique identifiers for all systems that handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) under contract performance. Contracting officers must confirm that a current CMMC status – at or above the required level for each system – is recorded in Supplier Performance Risk System (SPRS).

- **Clause Prescription.** DFARS 204.7504 was revised to clarify the phased implementation of CMMC requirements. The rule still imposes a phased rollout, focusing on Level 1 and Level 2 self-assessments in the first year; Level 2 third-party certifications in the second year; Level 3 certifications in the third year; and all contracts and solicitations will include CMMC requirements in the fourth year. In the first three years after the final rule’s effective date, application of the CMMC clauses in contracts is not required. However, the CMMC clauses may be included in contracts only if program managers choose to apply them. After that period, the clauses become mandatory for contracts involving contractor systems that process, store, or transmit FCI or CUI. The CMMC requirements do not apply to solicitations and contracts for commercial off-the-shelf items.
- **Solicitation Provision and Contract Clause.** The final rule adds specific CMMC-level options for the annual attestation. Additionally, offerors are ineligible for award without current CMMC status and affirmation of continuous compliance in SPRS for all relevant systems. Offerors must also submit their CMMC unique identifiers with proposals and update them as needed throughout contract performance. The final rule changes the term “senior company official” to “affirming official” to match 32 C.F.R. Part 170.
- **Reporting of Changes.** The final rule removes several proposed requirements to report to the contracting officer certain lapses in the contractor’s information security or CMMC certificate (or self-assessment) status during contract performance. Contractors will still be required to make timely notifications of information security incidents pursuant to DFARS 252.204-7012(c) and annual affirmations of continuing compliance.
- **Definitions.** Several key definitions are updated and added under DFARS 204.7501. “Current” is revised to reflect ongoing compliance with 32 C.F.R. Part 170 and to clarify its use in relation to different CMMC statuses – “Conditional CMMC Status,” “Final CMMC Status,” and “affirmation of continuous compliance.” “DoD unique identifier” is renamed “CMMC unique identifier.” New definitions are also added for “Federal contract information,” “plan of action and milestones” (POA&M), and “CMMC status” to ensure consistency and help contracting officers accurately assess compliance.

Implications for Government Contractors

- Contractors should continue preparations to conduct, at minimum, self-assessments against the Level 1 and Level 2 assessment controls, and should consider whether to schedule audits with certified assessment organizations to meet Level 2 third-party certification requirements. *Despite the phased rollout, DoD retains discretion to include certain CMMC-Level requirements during the phased approach.* Some programs may see Level 2 and Level 3 assessment requirements prior to the start of phases 2 and 3, respectively.
- Some contractors may see CMMC requirements included in contract modifications or at the exercise of an option. Contractors should review these documents carefully to ensure they understand their obligations, including affirmation of continuous compliance in SPRS.

- Contractors should pay careful attention to any CMMC requirements contained in solicitations, as the failure to have an appropriate CMMC level status will preclude a company from being awarded a contract. Challenges to CMMC requirements will likely need to be filed prior to the submission of proposals, and failure to make a timely challenge could prejudice a company.
- Subcontractors that receive FCI and/or CUI must also comply with the applicable CMMC flow-down requirements. DoD clarifies that it is up to the prime contractors to determine what information will be shared with their respective subcontractors and to ensure subcontractor compliance with the applicable CMMC requirements prior to subcontract award. Prime contractors should review their relationships with subcontractors and vendors in the operative supply chain to ensure visibility into CMMC statuses and proper reporting in SPRS.

The issuance of this rule completes the rulemaking required to implement the CMMC program, which was first proposed in September 2020. The final rule marks the culmination of a lengthy rulemaking process implementing the **CMMC program**. The phased rollout of CMMC requirement will begin Nov. 10, 2025.

Authors

This GT Alert was prepared by:

- **Eleanor M. Ross** | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- **Cassidy Kim** | +1 415.590.5133 | Cassidy.Kim@gtlaw.com
- **Olivia Bellini** | +1 703.903.7514 | Olivia.Bellini@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Berlin[~]. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Kingdom of Saudi Arabia⁺. Las Vegas. London^{*}. Long Island. Los Angeles. Mexico City⁺. Miami. Milan^{*}. Minneapolis. Munich⁻. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo[»]. Seoul[∞]. Shanghai. Silicon Valley. Singapore[~]. Tallahassee. Tampa. Tel Aviv[^]. Tokyo^{*}. United Arab Emirates[<]. Warsaw⁻. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ~Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. «Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legal Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ›Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ~Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¢Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ‹Greenberg Traurig's United Arab Emirates office is operated by Greenberg Traurig Limited. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2025 Greenberg Traurig, LLP. All rights reserved.*