KIRKLAND & ELLIS

Kirkland Alert

U.S. Defense Department Enhances Cybersecurity Requirements for Contractors

16 September 2025

On September 10, 2025, the U.S. Department of Defense[1] promulgated a final Rule amending the DFARS (the Defense Federal Acquisition Regulation Supplement) to incorporate the Cybersecurity Maturity Model Certification Program (CMMC) into DOD contracts, including, among other requirements, that certain contractors employ a third-party assessor to review their cybersecurity compliance. This Rule is set to take effect on November 10, 2025.

Overview of the CMMC Program and Rule Requirements

The CMMC program applies a tiered framework of cybersecurity requirements to defense contracts involving Controlled Unclassified Information (CUI) or Federal Contract Information (FCI), assigning contractors to one of three levels based on the sensitivity of the information they handle:

- **CMMC Level 1** applies to contractors that process, store or transmit FCI. These contractors must conduct an annual self-assessment and post the results in the Supplier Performance Risk System (SPRS), along with an annual affirmation of continuous compliance by an affirming official.
- **CMMC Level 2** is required for contractors handling CUI. Depending on the type of CUI involved, every three years, contractors will either be subject to a third-party assessment by a Certified Third-Party Assessment Organization (C3PAO) or will be permitted to conduct a self-assessment every three years. In both cases, an annual affirmation of compliance is required.
- **CMMC Level 3**, assigned to contracts involving the most sensitive information, requires contractors to undergo a DOD-led assessment every three years in addition to the Level 2 requirements.

With the exception of contracts solely for the acquisition of commercially available off-the-shelf (COTS) items, contractors must satisfy the requirements of their CMMC status in order to be awarded a contract, exercise an option or extend the period of performance. And contractors must maintain compliance throughout the life of the contract.

Phased Implementation

This Rule is subject to a phased three-year rollout. For the first three years, CMMC requirements will be included only in certain contracts as determined by program offices; after three years, CMMC requirements will apply to all contracts that will involve CUI or FCI (excepting COTS). The DOD estimates that this rule will impact 337,968 contractors and subcontractors by year four.

Conditional Status

This Rule offers contractors at CMMC levels 2 and 3 flexibility by awarding contracts with a conditional status for up to 180 days while the contractor actively works towards final CMMC status.

False Claims Act Implications

This Rule emphasizes the DOD's commitment to strengthening cybersecurity and aligns with recent efforts to enforce cybersecurity standards through the False Claims Act (FCA), which began with the U.S. Department of Justice's establishment of the Civil Cyber Fraud Initiative in October of 2021. The promulgation of this Rule follows recent settlements where the DOJ argued that defense contractors ignored cybersecurity deficiencies when self-assessing their compliance with relevant standards, such as the March 2025 settlement with MORSECORP Inc. The DOD emphasized its focus on cybersecurity in a recent statement. "We expect our vendors to put U.S. national security at the top of their priority list," said the acting DOD Chief Information Officer. "By complying with cyber standards and achieving CMMC, this shows our vendors are doing exactly that."

---

1. On Sept. 5, 2025, President Donald Trump issued an executive order, "Restoring the United States Department of War," to rename the DOD to the U.S. Department of War (DOW). ↩

Authors

Mark C. Holscher, P.C.

Partner / Los Angeles

Tammy A. Tsoumas

Partner / Los Angeles

Sofia Michael

Associate / Austin

Ethan Joel Levinton

Partner / Dallas

Sunil Shenoi

Partner / Chicago

Ivan A. Schlager, P.C.

Partner / Washington, D.C.

Evan Sills

Partner / Washington, D.C.

H. Boyd Greene IV

Partner / Washington, D.C.

Related Services

Practices

- Litigation
- Government Contracts

Suggested Reading

- 07 August 2025 Kirkland Alert Motor Finance — UK Supreme Court Allows Lenders' Appeal in Large Part; No Fiduciary or "Disinterested" Duty, but Possible Liability for "Unfair" Credit Terms
- 31 July 2025 Kirkland Alert Privy Council Abolishes the Shareholder Rule Under English Law
- 11 July 2025 Kirkland Alert Eighth Circuit Blocks FTC's Click-to-Cancel Rule