wiley

ALERT

DOD Issues Final DFARS Rule for Cybersecurity Maturity Model Certification Program

September 10, 2025

WHAT: The U.S. Department of Defense (DOD) has published the final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements for the Cybersecurity Maturity Model Certification Program (CMMC). The final rule at long last sets a starting date for phasing in the CMMC program.

WHEN: DOD issued the final rule on September 10, 2025, so 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 in the earlier final rule (which we summarized here) establishing the CMMC program requirements in Title 32 of the Code of Federal Regulations. *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.

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. Key updates include:

- DOD removed the requirement to notify the contracting officer of "lapses" in information security or changes in compliance.

Authors

Tracye Winfrey Howard
Partner
202.719.7452
twhoward@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

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

Teresita Regelbrugge
Associate
202.719.4375
rregelbrugge@wiley.law

Vaibhavi Patria
Associate
202.719.4667
vpatria@wiley.law

Practice Areas

Cybersecurity
Emerging Technologies
Government Contractors & Grantees
Government Contracts
Privacy, Cyber & Data Governance

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.

- DOD removed the term "data" and clarified that the rule would apply only to information that is Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).
- DOD incorporated definitions for FCI and Plan of Action and Milestones (PO&AM) from the FAR and Part 32 final rule on CMMC, respectively.
- DOD clarified the timeline for phased implementation of CMMC requirements.
- DOD confirmed that subcontractors also must submit affirmations of continuous compliance and the results of self-assessments in the Supplier Performance Risk System (SPRS). Prime contractors will not have access to subcontractor information in SPRS and will be responsible for ensuring that subcontractors meet the appropriate CMMC level for the information they will receive.

Stay tuned for our complete analysis of the final rule and compliance-related considerations. Wiley will also hold an upcoming webinar on CMMC.