



Cybersecurity Maturity Model Certification (CMMC)

Final rule sets CMMC rollout in motion



The long-awaited final rule ([48 Code of Federal Regulation "CFR"](#)) for the CMMC program was published in the Federal Register on September 10, 2025, and will become effective November 10, 2025¹. Once 48 CFR becomes effective, the official phased roll-out of CMMC will commence, spanning four phases over a three-year period. This structured approach culminates in the full implementation of CMMC requirements, with CMMC provisions included in all contracts by Phase 4 (November 2028).

NOTABLE TAKEAWAYS¹

- 1 Reporting requirement changes**
Reporting information security lapses or compliance changes under 32 CFR part 170 is no longer required, as Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012(c) addresses notification of security incidents.

Contractors must provide CMMC unique identifiers (UIDs) to Contracting Officers for all information systems that will process, store, or transmit federal contract information (FCI) or controlled unclassified information (CUI) during the contract. Additionally, any changes in the CMMC UIDs throughout the contract must also be reported to the Contracting Officer.
- 2 Subcontractor considerations for primes**
Prime contractors cannot access Supplier Performance Risk System (SPRS) details for subcontractors but remain responsible for verifying compliance. For example, prior to subcontract award, primes must confirm subcontractors have a requisite CMMC.

Subcontractors can share their CMMC status (such as a screenshot from SPRS) and copies of their certification as needed.
- 3 Inclusion of CMMC requirements in existing contract**
The Department of Defense (DoD) did not adopt recommendations to limit inclusion of CMMC requirements in existing contracts, emphasizing that modifications after the rule's effective date are at the contracting officer's discretion.
- 4 Clarification around FCI**
Added a definition for FCI based on the definition in Federal Acquisition Regulation (FAR) 52.204-21.

While the FCI definition indicates that "simple transactional information" does not constitute FCI, "information necessary to process payments" was given as an example of this type of non-FCI.
- 5 Clarification around conditional status**
For CMMC Levels 2 and 3 only, a conditional CMMC status may be granted for 180 days in accordance with 32 CFR 170.21, and award can be granted with a conditional CMMC level, however, closeout of plan of actions and milestones (POA&M) is needed for final CMMC status.

CONTACT US

Alan Faver

Partner
Deloitte & Touche LLP
afaver@deloitte.com

Charan Ahluwalia

Principal
Deloitte & Touche LLP
cahlwalia@deloitte.com

Keith Thompson

Managing Director
Deloitte & Touche LLP
kthompson@deloitte.com

Mika Alexoudis

Senior Manager
Deloitte & Touche LLP
malexoudis@deloitte.com

Federal Register, [Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements](#), September 10, 2025

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2025 Deloitte Development LLC. All rights reserved.