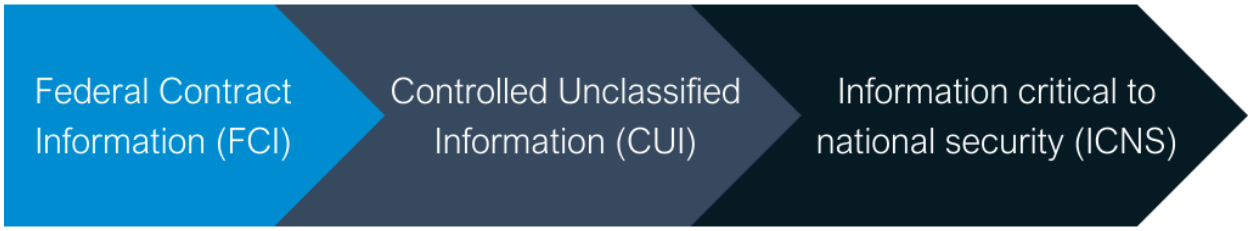
Department of Defense Proposes New Rule to Enforce Cybersecurity Standards Under CMMC 2.0

ARTICLE 09.17.24 KEVIN CORNWELL

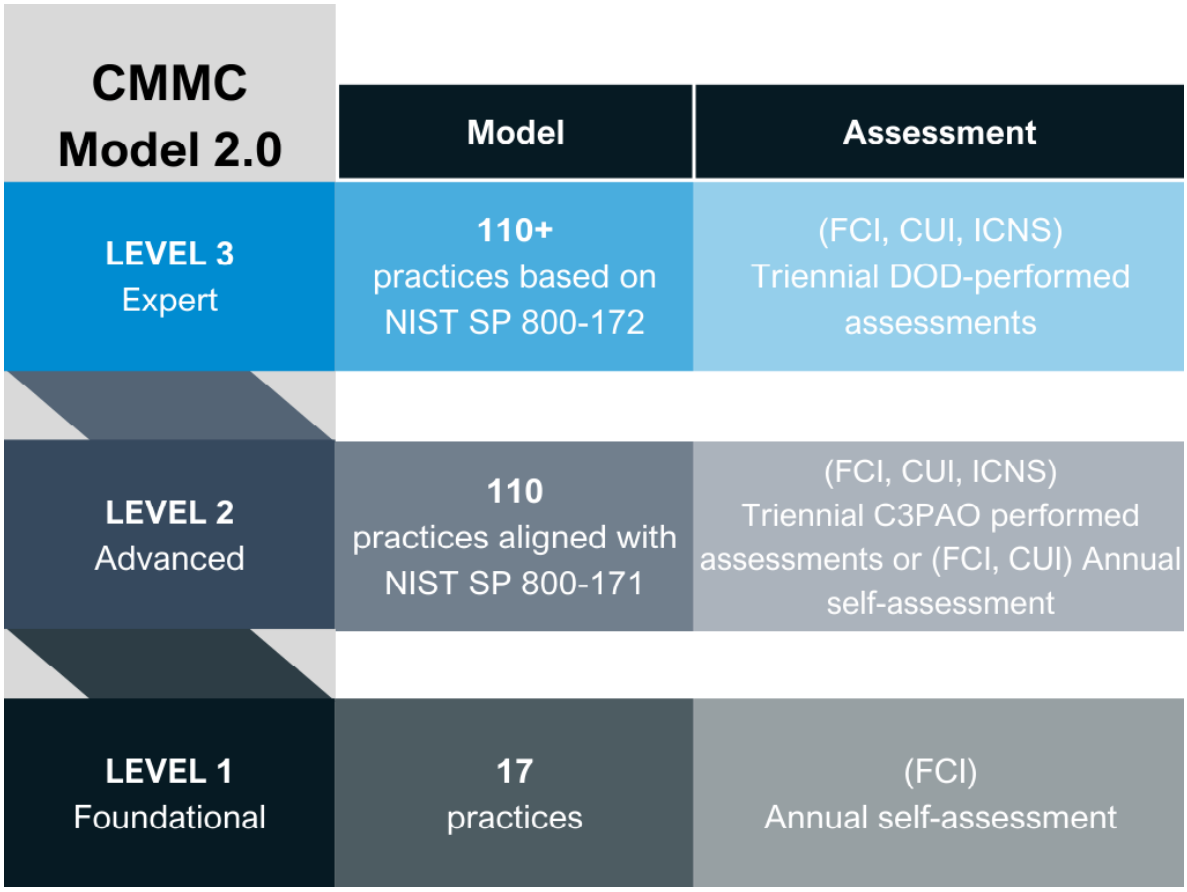
The Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0) has been out since 2022 but is not in effect nor has a clear timetable. However, it has been clear that Department of Defense (DOD) contractors were supposed to prepare for the compliance requirements. CMMC 2.0 got a step closer to reality in August 2024, in which the DOD introduced a proposed rule in the Federal Register that outlines the enforcement of its updated cybersecurity standards under CMMC 2.0. This proposal, which amends the Defense Federal Acquisition Regulation Supplement (DFARS), aims to integrate CMMC 2.0 requirements across all DOD vendor contracts involving the following forms of information.



The proposed rule does not appear to change anything we know about CMMC 2.0, but it clarifies some expectations and moves us closer to a finalized and effective date.

This new proposal introduces enhanced requirements for contracting officers. They will be responsible for ensuring bidders meet CMMC compliance and must notify contractors when CMMC standards apply to a contract.

CMMC 2.0 represents a significant overhaul of the original CMMC 1.0, launched in 2019, which faced criticism for its cost and restrictiveness. The updated model simplifies compliance by operating at three levels based on the type of information handled. Companies at Level 1 can conduct self-assessments, while some Level 2 entities can also self-assess, though others will need third-party certification from C3PAOs. Level 3 companies must obtain certification from the DOD.



The proposed rule stipulates that contractors must present a current CMMC certificate or self-assessment at the contract award stage. This requirement extends to subcontractors, who must comply with CMMC standards if they handle sensitive information.

Other notable provisions of the proposal:

- Contractors must maintain their CMMC level throughout the life of their contracts and affirm compliance annually or upon changes to their information systems.
- Contractors are required to submit unique DOD identifiers for each system processing, storing, or transmitting covered information.
- CMMC requirements must flow to subcontracts and other contractual instruments, extending compliance obligations broadly within the supply chain.
- Contractors must promptly notify contracting officers of any changes to their cyber systems or lapses in information security, with a 72-hour reporting window for significant changes.

The rule outlines a three-year phase-in period, during which CMMC requirements will initially apply to a subset of DOD contracts. Following this period, CMMC compliance will be mandatory for all relevant contracts. The public comment period for the proposed rule will close **on October 15, 2024**. If approved, the phased implementation could commence in 2025.