SPECIAL NOTICE

TYPE: Special Notice

Related Notice: INFOSEC ALERT - NOTICE TO THE USACE EUROPE DISTRICT INDUSTRIAL BASE

Title: UPDATE - Cybersecurity Maturity Model Certification (CMMC) 2.0 Implementation

SPECIAL NOTICE: Cybersecurity Maturity Model Certification (CMMC) Program Implementation UPDATE #3

Federal Organization Issuing Notice: U.S. Army Corps of Engineers (USACE), Headquarters, Directorate of Contracting

Description: DoD published the final CMMC rule on September 10, 2025, ref. 90 Federal Register (FR) 43560, with an effective date of **November 10, 2025**. This rule amends the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate CMMC requirements and partially implement Section 1648 of the FY20 NDAA, which directed the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the Defense Industrial Base (DIB). The rule adds a new solicitation provision (DFARS 252.204-7025, *Notice of Cybersecurity Maturity Model Certification Level Requirements*) addressing CMMC pre-award requirements, and revises the existing contract clause (DFARS 252.204-7021, *Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement[s])* to address new CMMC post-award requirements. DoD will implement CMMC in four phases:

- Phase 1 begins on November 10, **2025**.
- Phase 2 begins on November 10, **2026**.
- Phase 3 begins on November 10, **2027**.
- Phase 4, the final phase, begins on November 10, **2028**.

DoD's CMMC Program mandates that all organizations handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) maintain specific cybersecurity maturity levels to protect sensitive data. CMMC provides a consistent methodology to assess compliance with cybersecurity requirements and standards set forth in the 48 CFR 52.204-21; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Basic Safeguarding of Covered Contractor Information Systems.

As a reminder, CMMC focuses on organizations and systems that: **process, store, or transmit FCI or CUI, provide security for those systems, or are not logically or physically isolated from** those systems. CMMC safeguards apply to prime contractors and subcontractors at all tiers but are always based on sensitivity of the information. For example, CUI kept in paper form only does require physical safeguards yet does NOT trigger CMMC.

Prior to award of any contract or subcontract with a requirement for the CMMC Status of Level 1 (Self), the Organization Seeking Assessment (OSA) must both achieve a CMMC Status of Level 1 (Self) and have submitted an affirmation of compliance into SPRS for all information systems within the CMMC Assessment Scope.

For reference, the updated DFARS is available on DoD's Defense Pricing, Contracting, and Acquisition Policy (DPCAP) website.

Recommended Contractor Actions Now:

- Ensure your current cybersecurity posture aligns with contractual requirements related to NIST SP 800-171 controls.
- Follows all **steps** to use Procurement Integrated Enterprise Environment (PIEE) applications, to secure access to the Supplier Performance Risk System (SPRS) module and post a current self-assessment score in SPRS.
- Monitor updates from DoD, DPCAP, and SAM.gov for USACE Special Notices, official timelines and certification requirement updates.
- Comply with current DFARS 252.204-7012 requirements to report cyber incidents to DoD within 72 hours of discovery, using DoD's Cyber Crime Center (DC3) portal at: https://dibnet.dod.mil.

Important Disclaimers:

- This notice is for **INFORMATION ONLY** and **does not impose new requirements**.
- This notice does not create any rights/benefits enforceable by law against the U.S. Government.

Questions and Resources:

- **For USACE solicitations:** Contracting Officer/Contract Specialist listed on a SAM.gov post.
- **CMMC Program Resources:** https://www.acq.osd.mil/cmmc/
- **SPRS Training Classes and Tutorials:** https://www.sprs.csd.disa.mil/webtrain.htm
- **Regulatory References:** 32 CFR Part 170

NOTICE: THE CONTENTS OF THIS PUBLICATION DOES NOT HAVE THE FORCE OR EFFECT OF LAW AND IS NOT MEANT TO BIND THE PUBLIC OR GOVERNMENT IN ANY WAY. THIS NOTIFICATION IS SOLELY FOR INFORMATIONAL PURPOSES ONLY.