**SAM.GOV SPECIAL NOTICE**

**TYPE:** Special Notice

**Related Notice:** INFOSEC ALERT - NOTICE TO THE DEFENSE INDUSTRIAL BASE \*UPDATED\* (Published 31-JUL-2025)

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

**SPECIAL NOTICE:** UPDATE - Cybersecurity Maturity Model Certification (CMMC) 2.0 Implementation

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

**Description:**  The Department of Defense (DoD) finalized the Cybersecurity Maturity Model Certification (CMMC) 2.0 program on 16 December 2024. Once fully implemented, CMMC 2.0 will mandate that all DoD contractors and government organizations handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) achieve specific cybersecurity maturity levels to protect sensitive data. USACE and their Defense Industrial Base (DIB) contractors must comply with CMMC requirements for federal contracts and internal systems upon publication of the final Defense Federal Acquisition Regulations Supplement (DFARS) rule.

The CMMC Program establishes requirements for contractors and subcontractors to conduct an assessment of compliance with the applicable cybersecurity standard for contractor information systems that: **process, store, or transmit FCI or CUI; provide security protections for systems which process, store, or transmit CUI; or are not logically or physically isolated from systems which process, store, or transmit CUI.**

CMMC provides a consistent methodology to assess a defense contractor's implementation of required cybersecurity requirements using the security 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.*

**KEY HIGHLIGHTS FOR INDUSTRY**

* Like the DIB, USACE is awaiting final closure of four active DFARS cases related to CMMC. Reference: <https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf>.
  + DFARS Case 2023-D024, *Updates to the Safeguarding Covered Defense Information and Cyber Incident Reporting Clause*

Status: Report due date extended to 10/01/2025.

* + DFARS Case 2023-D021, *Information Technology, Cybersecurity, and Cyber-related Contractor Training and Certification Requirements*

Status: Report due date extended to 10/01/2025.

* + DFARS Case 2022-D017, *NIST SP 800-171 DoD Assessment Requirements*

Status: Draft final DFARS Rule; Report due date extended to 9/10/2025.

* + DFARS Case 2019-D041, *Assessing Contractor Implementation of Cybersecurity Requirements*

Status: 08/25/2025 Office of Information and Regulatory Affairs (OIRA) cleared final DFARS rule. Defense Acquisition Regulations System (DARS) Regulatory Control Officer preparing for publication, pending DoD Authority to Proceed (ATP).

* Upon final rule publication, the updated DFARS and PGI will be available on the Defense Pricing, Contracting, and Acquisition Policy (DPCAP) [website](https://www.acq.osd.mil/dpap/dars/change_notices.html).
* In accordance with [**Class Deviation 2025-O0006 – Use of the Clause on Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement**](https://www.acq.osd.mil/dpap/policy/policyvault/USA001756-25-DPCAP.pdf), USACE will not include the DFARS clause in new solicitations or contracts until publication of the new DFARS rule. Per the referenced deviation:

“New Solicitations and Contracts issued on or after [8/25/2025] will, to the maximum extent practicable, comply with Class Deviation 2005-O0006, requiring contracting officers *not* to use the contract clause at Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7021, *Contractor Compliance With the Cybersecurity Maturity Model Certification Level Requirement*, in new solicitations and contracts.”

* Note, if any new USACE solicitations or contracts, issued after 8/25/2025, included DFARS 252.204-7021, the DIB should anticipate an amendment or modification to remove the same.
* It is unclear at this time if active contracts will require contract modification upon publication of the DFARs rule. New regulatory guidance typically only applies to new solicitations and forward. However, we have no clear guidance on DoD’s planned implementation details currently.
* Expected Timeline: unknown. Original DoD guidance contemplated phased CMMC 2.0 implementation beginning 10/1/2025. However, the start date hinges on the rule publication date, which may be sooner or later than the original 10/1/2025 target.

**CONTRACTOR ACTIONS NOW:**

* Attend the INFOSEC [**Webinar**](https://events.dod.teams.microsoft.us/event/1b6a9efc-7c83-45b7-a238-8da725f79253@fc4d76ba-f17c-4c50-b9a7-8f3163d27582), scheduled and hosted by the U.S. Army Corps of Engineers on 9/17/2025 from 1300-1400 hours Central.
* Ensure your current cybersecurity posture aligns with contractual requirements related to NIST SP 800‑171 controls.
* Follows all [**steps**](https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml#step6) to use Procurement Integrated Enterprise Environment (PIEE) applications, to secure access to the Supplier Performance Risk System (SPRS) module, and post a current (no less than 3 years) 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**](https://dibnet.dod.mil).

**Important Disclaimers**

* This notice is for **INFORMATION ONLY** and **does not impose new requirements**.
* **CMMC 2.0 requirements** become enforceable only upon publication of the **final DFARS rule**.
* This notice does not create any rights/benefits enforceable by law against the U.S. Government.

**Questions and Resources**

* **For USACE solicitations:** contact the **Contracting Officer** or **Contract Specialist** listed on the relevant SAM.gov posting.
* **CMMC Program Resources:** <https://www.acq.osd.mil/cmmc/>
* **Regulatory References:** [32 CFR Part 170](https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/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.