



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

JUL 28 2025

**MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
DEFENSE AGENCY AND DOD FIELD ACTIVITY DIRECTORS**

SUBJECT: Resources for Implementing the Cybersecurity Maturity Model Certification Program

The Department of Defense (DoD or Department) is taking decisive action to enhance the security of DoD information in the possession of the defense industrial base (DIB) against escalating cyber threats. The DoD Chief Information Officer plays a vital role in this effort by overseeing the implementation of key initiatives, like the Cybersecurity Maturity Model Certification (CMMC) Program, designed to strengthen DIB defenses. CMMC is codified in Title 32 of the Code of Federal Regulations (CFR) Part 170 (32 CFR Part 170) and is a means to validate contractor compliance with information safeguarding requirements for federal contract information and controlled unclassified information. The purpose of this memo is to direct DoD Program Managers (PMs) and requiring activities to CMMC resources in anticipation of CMMC implementation.

32 CFR Part 170 describes all CMMC Program requirements. 32 CFR 170.3(e) outlines a phased timeline for inclusion of CMMC assessment requirements in DoD procurements and explains that, during the first 12 months of implementation, PMs and requiring activities should include CMMC self-assessment requirements in applicable solicitations and contracts. It is important to follow the recommended implementation plan to ensure industry has reasonable time to demonstrate compliance and become eligible for DoD contracts. Implementing higher-level CMMC assessment requirements ahead of the phased implementation timeline may reduce the pool of qualified contractors able to propose on competitive acquisitions, leading to reduced competition and potentially higher contract prices. Attachment 1 to this memo provides an overview of the phased implementation timeline.

My office, in coordination with the Undersecretary of Defense (USD) for Research and Engineering and the USD for Acquisition and Sustainment, published guidance to help PMs and requiring activities determine the appropriate CMMC assessment level to include in each solicitation and contract. The memo, which also outlines requirements for requesting and issuing CMMC assessment waivers, can be found here:
https://dodprocurementtoolbox.com/uploads/DOPSR_Cleared_OSD_Memo_CMMC_Implementation_Policy_d26075de0f.pdf.

In addition, my office has partnered with the Defense Acquisition University to develop several CMMC training courses for the defense acquisition workforce. Those interested can access these courses at <https://www.dau.edu/cybersecurity/cyber-solutions>.


Thank you for your continued partnership to strengthen DIB cybersecurity and protect DoD information.

CLEARED

For Open Publication

4
Aug 07, 2025

The point of contact for this matter is the CMMC Program Director, Mr. Buddy Dees at email: buddy.e.dees2.civ@mail.mil, or Ms. Carrie Cardwell at carrie.m.cardwell.civ@mail.mil.

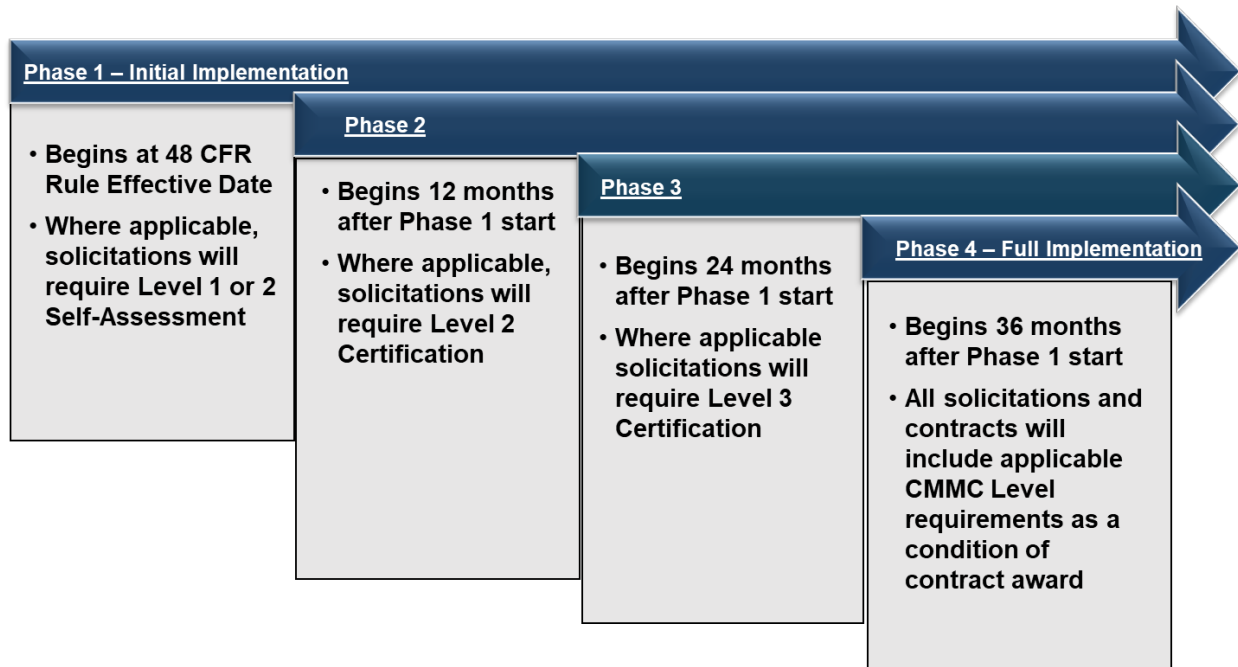
A handwritten signature in black ink, appearing to be 'KA' with a long horizontal stroke extending to the right.

Katherine Arrington
Performing the Duties of the
Chief Information Officer of the
Department of Defense

Attachment:
As stated

Attachment 1
Overview of Phased Timeline for CMMC Implementation

Phased Implementation of CMMC Requirements



In some procurements, DoD may implement CMMC requirements in advance of the planned phase