THE UNDER SECRETARY OF WAR
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION
AND SUSTAINMENT

JUL 13 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements

Rebuilding our military and reestablishing credible deterrence begins with putting the Department of War's (DoW) acquisition enterprise on a wartime footing and dramatically expanding and accelerating production and the fielding of new technology and advanced capabilities. To drive urgency and achieve acceleration in alignment with Executive Order 14265, Modernizing Defense Acquisitions and Spurring Innovation in the Industrial Base, which was signed in April 2025, the Department has transformed the way military requirements are developed, as well as refocused the Warfighting Acquisition System on five pillars under the Acquisition Transformation Strategy: (1) rebuilding the Arsenal of Freedom, (2) elevating and empowering the acquisition workforce to rapidly deliver capability, (3) maximizing acquisition flexibility through reduced regulations and process, (4) developing high performance systems through rigorous enterprise technical execution excellence, and (5) improving lifecycle risk management.

In alignment with Pillar 3, the DoW Chief Information Officer (CIO) has paused the rollout of the Cybersecurity Maturity Model Certification (CMMC) Program and suspended CMMC Phase 2 implementation. Program offices and requiring activities are only permitted to include CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement requests and requirement documents. The CMMC program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding Controlled Unclassified Information or Federal Contract Information. The DoW CIO is currently reviewing and reforming CMMC and is initiating a 60-day review to ensure that the Defense Industrial Base remains secure without imposing significant burden on the small and non-traditional businesses that are foundational to American manufacturing and innovation. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance as to which CMMC assessment levels may be applied during the program review and how to address solicitation and contract compliance concerns.

Michael P. Duffey

Attachment 1
Cybersecurity Maturity Model Certification Procedures

Per the attached CIO memorandum, during this suspension the Department will enforce baseline compliance with NIST SP 800-171 Rev 2 through CMMC Level 1 and CMMC Level 2 self-assessment and select Government-led assessments. The cybersecurity requirements outlined in the clause at DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, remain in effect.

- **Suspension of Phased Implementation Schedule, Including November 2026 Phase 2 Transition:** The upcoming November 2026 transition to Phase 2 of CMMC implementation is suspended. During the period of suspension, Program Managers and requiring activities must only include the need for CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement request and requirement documents. Program Managers and requiring activities may **not** designate CMMC Level 2 (C3PAO) or Level 3 (DIBCAC) assessments during this period. The allowed designations are CMMC Level 1 (Self) or CMMC Level 2 (Self).

    - **CMMC Level 1 Requirements**: CMMC Level 1 is a self-assessment requirement designed to provide insight into the offeror's compliance with the basic safeguarding requirements for Federal contract information (FCI) in the clause at FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems. This clause establishes the mandatory minimum safeguarding requirements for Federal contractors or subcontractors that have FCI residing in or transiting through their information systems.

    - **CMMC Level 2 Requirements**: Requiring activities may only include the CMMC Level 2 (Self) assessment requirement. CMMC Level 2 is aligned with NIST SP 800-171 Rev 2. The CMMC Level 2 self-assessment requirement is designed to provide insight into the offeror's compliance with security requirements for Controlled Unclassified Information (CUI). The Program Managers and requiring activities may require additional cybersecurity protections as commensurate with law and regulation.

- **Immediate Relief on Current Solicitations and Contracts:** If the original requirements package included a CMMC Level 2 (C3PAO) or CMMC Level 3 (DIBCAC) requirement, Program Managers and requiring activities **must** initiate amendments to active solicitations. They will provide an amended requirements document explicitly removing those requirements to the cognizant contracting officer or agreements officer, as applicable. The contracting officer or agreements officer must issue a corresponding solicitation amendment **as soon as practicable**. For existing contracts or agreements that already contain these requirements, contracting officers and agreements officers are directed to remove them via modification prior to the exercise of the next option period or during the next scheduled administrative modification.

- **Suspension of Waiver Procedures:** Program Managers and requiring activities must continue to identify information security requirements associated with a planned contract effort. Due to suspension of the CMMC Phase II implementation and the ability for program managers and requiring activities to select any CMMC requirements that would require CMMC Level 2 (3CPAO) or CMMC Level 3 (DIBCAC), no waivers shall be granted during the review of the program. This directive is effective immediately. Further guidance will be promulgated at the conclusion of the CIO's 60-day review.