DEPARTMENT OF WAR
6000 Defense Pentagon
Washington, D.C. 20301-6000

CHIEF INFORMATION OFFICER

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

SUBJECT: Removing Barriers to Defense Industrial Base Expansion: Immediate Suspension and Strategic Review of Cybersecurity Maturity Model Certification Requirements

The United States develops and manufactures the most lethal weapons systems in the world. To maintain this superiority and execute the Secretary of War's mandate to establish the Acquisition Transformation System (ATS) and place this Department on a wartime footing, we must ruthlessly eliminate bureaucratic barriers that impede our speed to capability delivery. While securing our networks against adversary intrusion remains a critical national security imperative, our approach must be realistic, business-enabling, scalable, and aligned with our broader strategic goals. The current iteration of the Cybersecurity Maturity Model Certification (CMMC) program, while intended to enhance security, imposes significant and often prohibitive burdens on the Defense Industrial Base (DIB), particularly the small and non-traditional businesses that are the engine of American innovation. While cybersecurity is essential, administrative compliance cannot come at the cost of warfighting capability and industrial base growth.

Recent data and feedback, including reports from the Small Business Administration, highlight that the current CMMC program is structurally incompatible with our need to rapidly expand the DIB. The combination of prohibitive compliance costs, severe shortages in third-party assessment capacity, and complex regulatory timelines is actively forcing innovative new entrants and small businesses to opt out of DoW contracts and freezing critical suppliers out of the market. The Secretary of War has directed the Department to lower barriers to entry, prioritize commercial-first mindsets, and leverage non-traditional procurement methods. Continuing to enforce CMMC deadlines under the current construct directly contradicts these directives, jeopardizing our ability to field capabilities to our warfighters. Our approach must be centered on achieving tangible supply chain and cybersecurity resilience, not one at the expense of the other.

To realign our cybersecurity posture with the principles of the ATS, we are directing the following immediate actions:

- Suspension of Upcoming Deadlines Including November 2026 Phase 2 Transition: The upcoming November 2026 deadline to transition to Phase 2 of CMMC implementation is suspended. Additionally, all pending and future CMMC implementation milestones across DoW solicitations and contracts are held in abeyance until further notice. Program Managers and requiring activities shall only include the need for CMMC Level 1 or Level 2 Self Assessments in procurement request and requirement documents. All other contractual cybersecurity clauses in contracts remain intact.

- CMMC Review and Reform Task Force: A dedicated CMMC Reform Task Force is to be immediately established to conduct a top-to-bottom 60-day review of the certification program. This Task Force will include cross-department representation to ensure a comprehensive review, and is charged with redesigning our supply chain cybersecurity approach to strictly align with the Secretary of War's ATS directives. The mandate of this Task Force is to provide recommendations for a reformed cybersecurity and operational resilience framework that prioritizes speed to capability, lowers barriers for small, medium, and non-traditional businesses, and replaces prohibitive, third-party compliance models with scalable, realistic security measures.

- Interim Cyber Posture: During this suspension, the Department will continue enforcing baseline compliance with NIST SP 800-171 Rev 2 through DIB self-assessments and select government-led assessments, focusing on tangible cyber hygiene rather than third-party certifications and bureaucratic, high cost-imposing red tape. The cybersecurity requirements outlined in DFARS clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting are still in effect. Existing DoW DIB cybersecurity services (i.e., DoW Cyber Crime Center services, NSA Cybersecurity Collaboration Center services, Office of Small Business Programs Project Spectrum) will continue to serve as no-cost resources to ensure companies are supported and business-enabled by meeting existing cyber requirements.

We will not defeat our adversaries with compliance checklists; we will defeat them by rapidly fielding superior capabilities produced by an expanded, resilient American industrial base.

This directive is effective immediately. Further guidance will be promulgated in the coming months.

Kirsten A. Davies