RELEASE

IMMEDIATE RELEASE

Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements

July 13, 2026

The Department of War today announces the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which were originally scheduled to come into effect on November 10, 2026. All Phase I self-assessment requirements remain firmly in place. Additionally, the Department will begin a comprehensive review of CMMC aimed at aligning with Secretary of War Pete Hegseth's Acquisition Transformation System (ATS) directives prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures.

Ensuring access to leading-edge commercial capabilities is a critical driver powering the Secretary of War's operational execution for the "Arsenal of Freedom". While the current CMMC program was designed to enhance DIB cybersecurity, instead it has created prohibitive compliance costs and bureaucratic burdens. Recent data, including reports from the Small Business Administration (SBA), confirmed that CMMC compliance is forcing innovative companies out of the Defense Industrial Base (DIB) which will delay the delivery of critical capabilities to the warfighters.

"In support of Secretary Pete Hegseth's directive to reduce compliance barriers for small and medium sized businesses, we are today suspending the CMMC Phase II requirements and initiating a 60-day study of the future of this program," said DoW Chief Information

Officer Kirsten A. Davies. "Robust cybersecurity and operational resilience remain critical to protecting American innovation and supporting warfighter readiness. We believe the DIB can achieve both, while we reduce unnecessary government red tape."

Effective immediately, the Department will suspend the transition to Phase II requirements of CMMC, as well as pending and future CMMC implementation milestones across the Department of War solicitations and contracts.

"We have a strategic imperative to reduce bureaucracy as we build the world's strongest Arsenal of Freedom. The CIO's decision ensures we maintain a strict security baseline while removing paralyzing costs and keeping innovators and competition growing in the defense supply chain," said Hon. Michael Duffey, Under Secretary of War for Acquisition and Sustainment.

To realign our cybersecurity posture with the principles of the ATS, the Department CIO is establishing a CMMC Reform Task Force to conduct a comprehensive top-to-bottom review of the certification program. This task force will serve as the central hub for synthesizing industry feedback from our public Request for Information (RFI) regarding compliance challenges. Using these insights, the team will recommend realistic, scalable security measures that prioritize speed to capability and lower barriers for small and non-traditional businesses, delivering their final report to the DoW CIO within 60 days.

During this interim period, the Department will enforce cybersecurity compliance with the NIST SP 800-171 Rev 2 standard through self-assessments and select government-led assessments, focusing on tangible cyber hygiene rather than administrative overhead.

It is critical to note that this action does not eliminate the requirement for companies to protect federal data. All defense contractors and subcontractors remain contractually obligated to safeguard covered defense information in accordance with DFARS clause 252.204-7012.

The Department of War remains steadfast in its commitment to securing its digital domain while empowering the DIB to rapidly provide the most advanced capabilities to the warfighter. More information can be found here: https://dowcio.war.gov/brilliantbasics