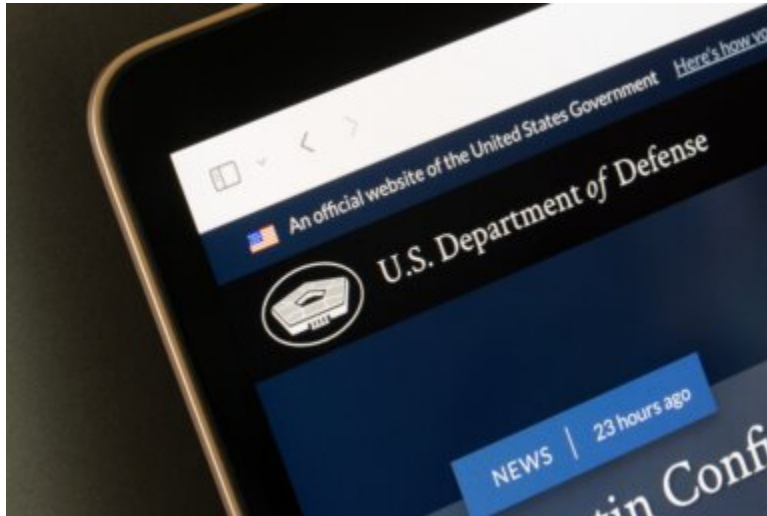


Pentagon Suspends CMMC Phase II Rollout: What Defense Contractors Need to Know



ARTICLE 07.14.26 KEVIN CORNWELL, CPA, CISA, CITP, CMMC RP

DoD Announces Review of the CMMC Program

On July 13, 2026, the U.S. Department of Defense (DoD) announced the suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which had been scheduled to take effect on November 10, 2026. According to the announcement, the Pentagon will conduct a comprehensive review of the CMMC program and evaluate the future direction of its implementation.

The decision reflects longstanding concerns surrounding the availability of accredited assessment organizations and the industry's capacity to support the large volume of contractors requiring certification. Many organizations—particularly small and mid-sized businesses within the Defense Industrial Base (DIB)—faced challenges securing assessment resources, creating the potential for significant certification backlogs.

Focus on Practical Cybersecurity and Reduced Administrative Burden

As part of the announcement, the DoD will establish a task force to conduct a 60-day review of the CMMC program. The review is expected to focus on strengthening tangible cybersecurity practices while reducing administrative complexity and compliance burdens for defense contractors.

For organizations that were preparing for a third-party CMMC Level 2 assessment, the suspension provides additional time while the DoD evaluates potential modifications to the program's structure and requirements.

What This Means for Defense Contractors

The most immediate impact is the postponement of the requirement to obtain a C3PAO (Certified Third-Party Assessment Organization) certification as a condition of contract award under the planned Phase II rollout. However, contractors should not interpret this announcement as a relaxation of cybersecurity obligations.

Important: Existing DFARS Requirements Remain in Effect

While CMMC certification requirements have been deferred, the cybersecurity requirements established under **DFARS 252.204-7012** remain fully in force. Organizations that store, process, or transmit **Controlled Unclassified Information (CUI)** are still expected to implement and maintain compliance with **NIST SP 800-171 Revision 2**.

The responsibility to protect CUI and demonstrate compliance with NIST SP 800-171 continues regardless of any temporary pause in CMMC certification requirements.

Recommended Actions During the Suspension

Organizations should continue advancing their cybersecurity programs rather than pausing compliance efforts. Key activities that remain critical include:

- Maintaining and updating System Security Plans (SSPs)
- Managing Plans of Action and Milestones (POA&Ms)
- Conducting periodic risk assessments
- Performing annual NIST SP 800-171 self-assessments
- Maintaining documentation and evidence of compliance
- Addressing known control gaps and remediation activities
- Strengthening cybersecurity governance and oversight

These efforts support current contractual obligations and will position organizations for success regardless of the future evolution of the CMMC program.

Should Organizations Delay a C3PAO Assessment?

Given the uncertainty surrounding future certification requirements, some organizations may choose to postpone a formal C3PAO certification assessment. However, there is still significant value in pursuing readiness activities.

Many C3PAOs offer **mock assessments** that simulate the rigor of an official evaluation. These exercises can help organizations validate their implementation of NIST SP 800-171 controls, identify gaps, and strengthen audit readiness.

This preparation remains especially important because the DoD continues to conduct NIST SP 800-171 assessments through its **Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)** teams. A mock assessment can provide valuable assurance that cybersecurity controls are operating effectively and can withstand a government assessment.

Looking Ahead

The DoD's review may ultimately reshape how CMMC is implemented, but the underlying expectation remains unchanged: defense contractors must protect sensitive information and maintain strong cybersecurity practices.

Organizations should continue investing in cybersecurity maturity, compliance documentation, and control effectiveness while monitoring developments from the Department of Defense.

If you would like to discuss how this announcement may affect your organization's compliance strategy, assessment plans, or NIST SP 800-171 readiness efforts, [please contact our team](#).