wiley

ALERT

DOD Pauses CMMC 2.0 Implementation: A Big Deal with Little Immediate Impact

July 17, 2026

WHAT: On July 13, 2026, the U.S. Department of War/Defense (DOD or Department) suspended the Phase II requirements of the Cybersecurity Maturity Model Certification (CMMC) Program, which were expected to take effect on November 10, 2026 (press release). The CMMC Program has implemented Phase I. As a result, procuring activities must include the requirements of CMMC Level 1 and Level 2 (Self Assessments) in solicitations and contracts when DOD anticipates the contractor may handle Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). Before DOD issued this suspension, as discussed below, DOD would have been required under Phase II to also include requirements for Level 2 with assessments by CMMC third-party assessor organizations (C3PAOs).

DOD is also soliciting industry feedback to inform a new effort to reform the CMMC program through a Request for Information (RFI) here. Responses must be submitted by email and will be accepted until 12:00 p.m. Eastern time on Friday, August 14, 2026.

WHAT DOES THIS MEAN FOR INDUSTRY: Most cybersecurity requirements applicable to DOD contracts—including the need to safeguard FCI and CUI, to implement the 110 security controls prescribed in NIST 800-171, to rapidly report cyber incidents, and to certify compliance—arise outside of the CMMC Program. This development, thus, has no impact on those existing requirements. Nor does it affect the U.S. Department of Justice's (DOJ) commitment, through its Civil Cyber-Fraud Initiative, to pursue False Claims Act cases against those who do not comply with existing, non-paused requirements. Within the CMMC program, the requirement to conduct a self-assessment will remain an obligation during this pause. This pause delays only the mandatory requirement for a C3PAO

Authors

Kara M. Sacilotto
Partner
202.719.7107
ksacilotto@wiley.law

Gary S. Ward
Partner
202.719.7571
gsward@wiley.law

Erin M. Joe
Special Counsel
202.719.3140
ejoe@wiley.law

Nova J. Daly
Senior Advisor
202.719.3282
ndaly@wiley.law

Teresita R. Kummer
Associate
202.719.4375
rkummer@wiley.law

Practice Areas

Government Contractors & Grantees
Government Contracts
Privacy, Cyber & Data Governance
Trump Administration Resource Center

assessment, which otherwise would have taken effect in November.

Yet the pause is still significant because it reflects a concrete step away from the status quo, surfacing a disagreement that has been simmering within the Government since the beginning of the second Trump Administration about how to balance DOD's security needs with the burden on industry. Industry got a public glimpse of this disagreement last year when President Trump issued a deregulatory agenda in March 2025 that cited DOD's CMMC Rule as an "other notable costly Biden Administration regulation[]" that carried a $42.26 billion impact. But six months later, DOD finalized this rule without significant changes, finally setting the CMMC Program into operation. This appeared to settle the debate that CMMC was here to stay. But this announcement changes that course in that it previews at least the possibility of changes to the existing cybersecurity requirements beyond CMMC.

BACKGROUND

DOD has spent over a decade shaping the CMMC program. Shortly after the Government first coined the term CUI in 2010, DOD announced its earliest plans to add standard contract requirements for safeguarding this type of information in the DFARS. Cybersecurity requirements have taken various forms, including the safeguarding of Covered Defense Information (CDI), cyber incident reporting and flow down requirements at DFARS 252.204-7012, the subsequent certification and DOD assessment requirements in DFARS 252.204-7019 and -7020, and the CMMC framework in DFARS 252.204-7021.

DOD established the CMMC Program in two different parts of the Code of Federal Regulations. The "Program Rule," codified at 88 Fed. Reg. 89058, established the substantive framework for the CMMC program, including the varying levels, security requirements, and certification processes. The "DFARS Rule," codified at 89 Fed. Reg. 83092, established requirements for contracting officers, including the contents of the standard clauses that contracting officers will be required to include in all covered contracts.

A Refresher on CMMC Program Requirements and Timeline

The CMMC Program requires contractors that process, store, or transmit FCI or CUI in performance of a DOD contract to adopt substantive security requirements based on the CMMC Level determined for that effort. There are three CMMC Levels, depending on the sensitivity of the information and program at issue:

- **Level 1** applies when the contractor's information systems will process, store, or transmit FCI but not CUI;
- **Level 2** applies when the contractor's information system will process, store, or transmit CUI; and
- **Level 3** applies when the contractor will support DOD's most critical programs and technologies.

In addition to implementing the relevant technical requirements, the CMMC Program requires contractors to periodically assess compliance for each covered information system and annually submit an affirmation of continuous compliance with CMMC requirements through DOD's Supplier Performance Risk System (SPRS).

- For CMMC Level 1 (Self) or Level 2 (Self), contractors are required to perform a self-assessment and post the score in the SPRS.
- For CMMC Level 2 (C3PAO), contractors must undergo a third-party assessment from a C3PAO. A C3PAO assessment is valid for three years.
- For CMMC Level 3, contractors must obtain a C3PAO assessment confirming compliance with the Level 2 requirements and a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) certification confirming compliance with the 24 additional security requirements from NIST 800-172. Each assessment is valid for up to three years.

The CMMC Program had four implementing phases. Phase I began on November 10, 2025. As of that date, DOD would include requirements for CMMC Level 1 (Self) or Level 2 (Self) in applicable solicitations and contracts. During Phase I, DOD also has the discretion to include a requirement for Level 2 (C3PAO), but is not required to do so.

Phase II was set to kick off on November 10, 2026. For Phase II, DOD would have required Level 2 (C3PAO) certification assessments for all applicable solicitations and contracts. DOD also would have had discretion to include the requirement for CMMC Level 3 (DIBCAC) for applicable solicitations and contracts.

Phase III is to begin a year following Phase II, and would require that DOD include Level 3 (DIBCAC) requirements in all applicable solicitations and contracts. It was planned that by November 10, 2028, the CMMC Program would be fully implemented and all CMMC requirements would be included in applicable solicitations, contracts, and exercises of option periods. That timeline is now in question.

FOCUS OF REFORM AND THE REQUEST FOR INFORMATION

The Department's Chief Information Officer (CIO) and Undersecretary for Acquisition & Sustainment each issued a memorandum to implement the suspension of CMMC Phase II requirements (and). Based on those memoranda and the Department's press release, the CIO will establish a CMMC Reform Task Force to conduct a 60-day review of the CMMC Program to align CMMC with Secretary Pete Hegseth's Acquisition Transformation Strategy (ATS) directives to prioritize speed to capability, lower barriers for small, medium, and non-traditional businesses, and replace bureaucratic compliance with scalable, resilient cybersecurity measures. The suspension announcement refers to recent reports by the Small Business Administration (SBA) regarding the burdens that the CMMC Program has imposed on small and non-traditional businesses. The SBA issued a news release commending the suspension and referencing compliance burdens reaching "over 100,000 small businesses" and individual company compliance costs to obtain CMMC certification "approaching as much as $600,000."

The RFI poses seven questions inviting industry input regarding:

- Cost drivers, administrative burdens, or operational challenges with complying with CMMC and NIST SP 800-171 Rev 2;

- Which security controls industry has found to deliver greater cybersecurity and risk reduction;
- Which security controls create the greatest administrative and financial burdens, while offering only limited improvements;
- Commercial cybersecurity capabilities, platforms, and services that DOD could better recognize or accept within a cybersecurity compliance framework;
- How Phase I self-assessments could be streamlined;
- Have self-assessments led to a more dynamic cyber posture or are they only performed for compliance purposes; and
- Actionable policy changes or regulatory reforms that could reduce costs and barriers to entry for small, medium, and non-traditional businesses or would improve operational resilience against cyber attacks.

DOD intends that responses to the RFI inform upcoming policy reforms aligned with Executive Order 14265, *Modernizing Defense Acquisitions and Spurring Innovation in the Industrial Base* signed in April 2025, and the ATS directives "prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures," according to the suspension announcement.

KEY TAKEAWAYS

Safeguarding, Cyber Incident Reporting, Attestation, and Self-Assessment Requirements Remain. Contractors are still required to safeguard FCI and CUI, rapidly report cyber incidents, complete self-assessments, post scores to SPRS, and provide annual affirmations of continuous compliance even during the suspension of CMMC Phase II requirements. The CIO affirmed that the requirements under contract clause DFARS 252.204-7012 remain in effect and that the Department will continue to enforce compliance with NIST SP 800-171 Rev 2 through self-assessments and select government-led assessments even during the Phase II suspension. The current suspension merely pauses the need for all new contracts to require a C3PAO certification.

Amendments to Active Solicitations and Contracts Forthcoming. The Department intends to require activities to amend active solicitations to remove CMMC Phase II requirements "as soon as possible" and has also directed contracting officers to issue modifications to remove those requirements from existing contracts prior to the exercise of the next option period or the next scheduled administrative modification.

Potential Adjustments to CMMC Scope. DOD's Press Release and RFI seem to suggest a significant reevaluation of the CMMC Program. The CMMC rulemaking took an approach that, in order to best safeguard federal data, CMMC requirements should reach contractors and subcontractors of all sizes, across all contract types (except COTS procurements). The suspension signals that a shift in the CMMC Program's scope may be forthcoming, whether that includes allowing industry more flexibility to shape cybersecurity through broadening commercial solutions and organizationally defined parameters, or reframing requirements for smaller and non-traditional entities. But changes on this scale would require corresponding changes to several other regulations, as noted below.

What about NIST SP 800-171 Rev.3 and the FAR CUI Proposed Rule? As DOD pumps the brakes on CMMC, other entities within the Government have sent conflicting signals. Just last month, the FAR Council updated its proposed rule that would expand similar safeguarding and incident reporting requirements to all CUI handled under all federal contracts (issued on June 23, 2026, and covered here). Comments on the FAR proposed rule are due by July 23. If the FAR proposed rule is implemented as drafted, a reduction in scope of requirements under the CMMC framework may not offer much relief for those contractors who would be implementing the requirements of the FAR CUI rule regardless.

Prepare Your Supply Chain. Many contractors and subcontractors have already spent years preparing for CMMC Phase II implementation. While this latest signal from DOD is worth monitoring, it is too soon to call these efforts off. CMMC 2.0 is not off the table yet; the underlying requirements remain largely in place, and what comes next may be even more unpredictable.

* * *

Wiley's cross-disciplinary Government Contracts, National Security, and Privacy, Cyber & Data Governance teams have extensive experience advising clients on all aspects of compliance with CMMC requirements and will continue to monitor these developments