SQUIRE PATTON BOGGS

Department of Defense suspends CMMC Phase II implementation and seeks industry input on future reforms

On July 13, 2026, the Department of Defense (DoD) Chief Information Officer (CIO) suspended implementation of the Cybersecurity Maturity Model Certification (CMMC) Phase II and launched a CMMC Review and Reform Task Force to reassess the CMMC program, reduce compliance burdens, and gather direct industry feedback regarding future cybersecurity requirements.

Based on the recently issued suspension memorandum and accompanying request for information (RFI), defense contractors should evaluate the potential impact on their compliance strategies and consider participating in the comment process.

Key dates

Date	Event
July 13, 2026	CIO memorandum suspends CMMC Phase II implementation pending a 60-day review of the program.
July 13, 2026	DoD issues an RFI titled "Reforming CMMC and Reducing Compliance Burden for the Defense Industrial Base" and announces the formation of a CMMC Reform Task Force.
August 14, 2026 (Noon ET)	Deadline for industry responses to the RFI.
November 2026	Previously scheduled implementation of CMMC Phase II is suspended.

What was Phase II going to require?

Prior to the suspension, CMMC Phase II was scheduled to take effect in November 2026 and would have expanded assessment requirements beyond self-attestation for certain contractors handling Controlled Unclassified Information (CUI).

The suspension memorandum specifically halts the transition to requirements involving:

- CMMC Level 2 certification through a certified third-party assessment organization (C3PAO)
- CMMC Level 3 assessments conducted by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

As a result, contractors currently remain subject only to self-assessment requirements, unless and until the Department issues revised guidance following the task force review.

What does the suspension mean?

During the suspension period:

- The planned November 2026 CMMC Phase II implementation will not occur.
- Agencies may only require:
  - CMMC Level 1 (Self-Assessment) for Federal contract information (FCI)
  - CMMC Level 2 (Self-Assessment) for CUI.
- Program offices may not require:
  - CMMC Level 2 (C3PAO) certification assessments
  - CMMC Level 3 (DIBCAC) certification assessments
- Existing solicitations containing CMMC Level 2 (C3PAO) or CMMC Level 3 (DIBCAC) requirements must be amended to remove those requirements as soon as practicable.

- Existing contracts containing those requirements are to be modified prior to option exercise or during the next administrative modification.
- The underlying cybersecurity obligations in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," and the requirements associated with National Institute of Standards and Technology Special Publication (NIST SP) 800-171 Rev. 2, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," remain in effect.

Should you submit comments?

The Department is seeking feedback from defense industrial base (DIB) participants regarding:

- Cost drivers and administrative burdens associated with CMMC and NIST SP 800171 compliance
- Security controls that provide meaningful cybersecurity improvements
- Regulatory requirements that create excessive cost and administrative burden with limited cybersecurity benefit
- How the DoD can recognize the effective use of commercial cybersecurity tools, platforms and managed services
- Challenges associated with self-assessments and reporting
- Policy changes that the CMMC Reform Task Force should recommend to reduce compliance burdens while maintaining cybersecurity protections
- Policy changes that the CMMC Reform Task Force should recommend to improve operational resilience against cyberthreats.

The Department has expressly stated that feedback from DIB participants will be used to inform recommendations developed by the newly formed CMMC Reform Task Force. The outcome of this review could significantly influence the future structure of CMMC requirements, third-party assessment obligations, self-attestation processes, and broader cybersecurity compliance expectations for defense contractors.

Conclusion

Organizations that have experienced significant compliance costs, assessment challenges, or operational burdens under the current CMMC framework should strongly consider participating in the RFI process. Our government contracting team can assist clients in evaluating the suspension's impact and drafting strategic responses to the RFI before the August 14, 2026, deadline.

Contacts

Karen Harbaugh
Partner, Washington DC
T +1 202 457 6485
karen.harbaugh@squirepb.com

Jeremy W. Dutra
Partner, Washington DC
T +1 202 626 6237
jeremy.dutra@squirepb.com

Patrick Madrid
Associate, Washington DC
T +1 202 457 5260
patrick.madrid@squirepb.com

71801/07/26