APEX
NORTHWEST TEXAS APEX ACCELERATOR CENTERS

CMMC Phase II Put on Hold: What Federal Contractors Should Know

by Huey Lee

The Department of War announced on July 13, 2026, that it is suspending the transition to Phase II of the Cybersecurity Maturity Model Certification program, commonly known as CMMC.

Phase II was scheduled to begin on November 10th and would have expanded the use of third-party CMMC Level 2 assessments for contractors handling Controlled Unclassified Information.

For many small defense contractors, the announcement provides temporary relief from the cost and preparation involved in obtaining third-party certification. However, it is important to understand what the suspension does and does not change.

CMMC has not been eliminated

The suspension does not end the CMMC program. Instead, the Department will remain under Phase I while it conducts a comprehensive review of the program.

(scroll down to keep reading...)

During the suspension, Department of War program managers and requiring activities may only designate:

- CMMC Level 1 self-assessments
- CMMC Level 2 self-assessments

They may not designate CMMC Level 2 assessments performed by a Certified Third-Party Assessment Organization, or C3PAO, or Level 3 assessments performed by the Defense Industrial Base Cybersecurity Assessment Center.

The Department has also directed contracting personnel to amend active solicitations containing Level 2 C3PAO or Level 3 requirements. For existing contracts, those requirements are to be removed through a contract modification, generally before the next option period or during the next scheduled administrative modification.

Contractors should watch for the actual amendment or modification rather than assume a requirement has already been removed.

Cybersecurity requirements remain in effect

Although Phase II is suspended, contractors must continue protecting sensitive federal information.

DFARS 252.204-7012 remains in effect. When this clause applies, contractors must continue to safeguard Covered Defense Information, comply with applicable requirements in NIST SP 800-171 Revision 2, and report covered cyber incidents.

Depending on the contract and the information involved, a contractor may still need to:

- Protect Federal Contract Information, or FCI
- Protect Controlled Unclassified Information, or CUI
- Maintain a System Security Plan
- Complete a Level 1 or Level 2 self-assessment
- Submit an assessment score and required affirmations through the Supplier Performance Risk System
- Maintain documentation supporting its assessment
- Participate in a selected government-led assessment

Continued...

A self-assessment should be based on the company's actual cybersecurity practices. Contractors should not claim that a security requirement has been implemented unless they can support that claim with appropriate documentation and evidence.

Why did the Department suspend Phase II?

According to the Department, the cost and administrative burden of third-party certification were creating barriers for small, medium-sized, and non-traditional businesses. The Small Business Administration also expressed concern that these burdens were causing some companies to leave or reconsider participating in the Defense Industrial Base.

The Department has established a CMMC Reform Task Force to review the program and recommend changes. The review will consider how to maintain strong cybersecurity while reducing unnecessary costs and making compliance more practical and scalable.

The Department is also requesting industry feedback on subjects such as:

- The largest CMMC compliance costs and administrative burdens
- Security controls that provide the greatest reduction in actual cyber risk
- Requirements that create significant costs without comparable security benefits
- The use of commercial cybersecurity tools and managed services
- Ways to simplify self-assessment and reporting
- Reforms that could reduce barriers without weakening protection of federal information

Comments responding to the Request for Information are due August 14, 2026.
(see links to the official memo and guidance at the end of this article.)

Continued...

What should contractors do now?

Defense contractors should continue preparing to meet the cybersecurity requirements that apply to their work. Suspending Phase II does not remove the responsibility to protect government information.

Companies should take the following steps:

1. **Review each solicitation and contract.** Identify the CMMC, DFARS, and cybersecurity requirements that are actually included.
2. **Continue NIST SP 800-171 implementation.** Do not stop cybersecurity improvements solely because Phase II has been suspended.
3. **Keep documentation current.** Maintain the System Security Plan, assessment records, policies, procedures, and evidence supporting the company's cybersecurity practices.
4. **Monitor SPRS requirements.** Verify that required assessment scores and annual affirmations are accurate and current.
5. **Look for contract amendments or modifications.** If a solicitation or contract currently requires a C3PAO or Level 3 assessment, contact the contracting officer for clarification.
6. **Communicate with prime contractors.** Subcontractors should ask whether a prime contractor's requirements have changed. A prime may have its own cybersecurity expectations in addition to the requirements established by the government.
7. **Use caution before canceling a scheduled C3PAO assessment.** First determine whether the customer still expects the assessment, whether cancellation fees apply, and whether certification would provide a business advantage.

The bottom line

CMMC Phase II and its expanded third-party certification requirements have been suspended, but CMMC has not gone away. Phase I self-assessments remain in effect, and contractors must continue meeting the cybersecurity requirements contained in their solicitations and contracts.

The CMMC program may change after the Department completes its review.

Continued...

Contractors should continue strengthening their cybersecurity programs, monitor official announcements, and avoid making major compliance decisions based solely on headlines.

For official information, visit the Department of War CMMC website and review the Department's CMMC Phase II implementation guidance.

Read the official memos. Comments responding to the Request for Information are due August 14, 2026.

The Northwest Texas APEX Accelerator provides general government-contracting education and assistance. This information should not be considered legal, cybersecurity, or regulatory-compliance advice.

Need help with your CMMC Self-Assessment?

Contact someone on our team!

APEX
NORTHWEST TEXAS APEX ACCELERATOR CENTERS

Huey Lee, Advisor
Huey.Lee@ttu.edu
(806) 834-2540
Cybersecurity Lead

Brandy Reed, Advisor
Brandy.Reed@ttu.edu
(806) 834-2868

David Miller, Advisor
David.B.Miller@ttu.edu
(806) 834-3769

Rich Lyles, Director
Rich.Lyles@ttu.edu
(806) 834-7459