CMMC Phase II Suspension

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

CMMC Phase II Suspension

On July 13, 2026, the Department of Defense (DoD) announced the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II implementation requirements that were scheduled to take effect on November 10, 2026. Specifically, the DoD has paused the requirement for many contractors handling Controlled Unclassified Information (CUI) to obtain a certification from a Certified Third-Party Assessment Organization (C3PAO). The Department simultaneously established a 60-day CMMC Reform Task Force to perform a comprehensive review of the program and recommend changes.

While this announcement significantly affects certification timelines and assessment planning, it does not eliminate contractors' cybersecurity obligations under DFARS, NIST SP 800-171, or existing CMMC self-assessment requirements. The technical requirements remain largely unchanged; only the third-party validation mechanism has been suspended pending further review. The Cyber AB and the DOD are still processing and tracking the results of third-party assessments and issuing certificates for Organizations Seeking Certification (OSC).

What Has Changed

CMMC Phase II Has Been Suspended

Prior to the announcement, CMMC Phase II was scheduled to begin on November 10, 2026. Under Phase II, contractors handling CUI would have been required to obtain an independent assessment conducted by a C3PAO before award of certain contracts.

The DoD has now suspended this transition indefinitely while conducting a comprehensive review of the program. Acquisition officials have been directed not to include Level 2 C3PAO assessment requirements during this suspension period. While the DoD has suspended the third-party assessments, there has been conversation that the 5 major primes are meeting to possibly establish their own requirements.

Existing Solicitations and Future Requirements Are Being Revised

The DoD has directed contracting activities to amend solicitations and future procurement packages that included C3PAO requirements, substituting self-assessment requirements where appropriate until further notice.

What Remains Required

Despite widespread discussion that "CMMC has been paused," defense contractors should understand that the majority of cybersecurity obligations remain fully in effect.

NIST SP 800-171 Compliance

Organizations that process, store or transmit CUI remain responsible for implementing the 110 security requirements in NIST SP 800-171 Rev. 2. The suspension does not relax these controls or diminish the expectation that contractors achieve compliance.

DFARS 252.204-7012 Requirements

The following DFARS obligations remain unchanged:

- Protection of Covered Defense Information (CDI)
- NIST SP 800-171 implementation
- Cyber incident reporting
- Media preservation requirements
- Flow-down requirements to subcontractors

The DoD explicitly stated that the suspension does not eliminate legal obligations to safeguard federal information.

SPRS Self-Assessment Reporting

Phase I requirements of the CMMC program that became effective in November 2025 are still active and contractors remain responsible for:

- Performing self-assessments
- Calculating SPRS scores
- Maintaining supporting documentation
- Updating assessments as required

System Security Plans and Documentation

Contractors should continue maintaining:

- System Security Plans (SSPs)
- Asset inventories
- Network diagrams
- CUI data flow diagrams
- Shared Responsibility Matrices
- Plans of Action and Milestones (POA&Ms)

These artifacts remain foundational requirements for demonstrating compliance with NIST SP 800-171 and for eventual certification when or if third-party assessments return. Consistent with Schneider Downs' CMMC methodology, these documents remain critical readiness artifacts.

Areas Currently in Flux

Future of Third-Party Certification

The largest unresolved issue is whether mandatory C3PAO assessments will:

- Return in their current form;
- Be delayed;
- Be modified to reduce cost and complexity;
- Be replaced with an alternative validation model; or
- Be significantly scaled back for certain segments of the Defense Industrial Base.

The DoD has not announced a final direction and is soliciting feedback from the ecosystem via a RFI published on July 14th.

Long-Term CMMC Structure

The Task Force has been directed to develop recommendations that reduce administrative burden while maintaining cybersecurity protections. Several public reports indicate the DoD is evaluating alternatives to the current third-party assessment framework.

Contractual Enforcement Strategy

Questions remain regarding:

- Whether future contracts will require self-attestation only;
- Which organizations may still need independent assessments;
- How subcontractor requirements will evolve;
- Whether DIBCAC-led Level 3 assessments will proceed as originally envisioned.

No formal guidance has yet been issued regarding these topics.

Existing Assessment Investments

Contractors currently preparing for certification face uncertainty regarding:

- Timing of future assessments;
- Value of scheduled readiness reviews;
- C3PAO assessment demand forecasts; and
- Availability of certification pathways after the review concludes.

The DoD review is expected to provide additional guidance, but no outcome has been announced.

Recommended Actions for Contractors

Until further guidance is issued, contractors should:

- Continue implementing NIST SP 800-171 controls;
- Maintain and improve SPRS scores;
- Complete SSPs, network diagrams and CUI scoping activities;
- Continue readiness assessments and gap remediation efforts;
- Treat the suspension as schedule relief rather than a compliance exemption; and
- Monitor DoD communications regarding the 60-day CMMC Reform Task Force review.

Organizations that pause cybersecurity improvement efforts based on the suspension may find themselves unprepared if the DoD reintroduces an assessment mandate in a revised form. Multiple industry sources have emphasized that the substantive cybersecurity requirements remain intact even though the independent assessment requirement has been paused.

Bottom Line

The DoD has suspended the requirement for most CMMC Level 2 third-party assessments, but it has not suspended the cybersecurity requirements that underpin CMMC. Contractors handling CUI remain obligated to implement NIST SP 800-171 controls, maintain required documentation, perform self-assessments, report SPRS scores and comply with DFARS cybersecurity requirements. The principal uncertainty is no longer what security controls are required but rather how and when compliance will ultimately be validated.

About Schneider Downs IT Risk Advisory

Our IT Risk Advisory practice helps ensure that your organization is risk-focused, promotes sound IT controls, ensures the timely resolution of audit deficiencies and informs the board of directors of the effectiveness of risk management practices. We will partner with you to provide comprehensive IT audits and compliance reviews that will ensure your organization has effective and efficient technology controls that better align the technology function with their business and risk strategies.

To learn more, visit our IT Risk Advisory page or contact us at contactsd@schneiderdowns.com.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX
AUDIT AND ASSURANCE
CONSULTING
WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

METROPOLITAN WASHINGTON
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003