

CMMC Paused the Certification Clock. Your Customer Requirements Kept Moving.

Phase 2 is suspended, but applicable self-assessments, NIST SP 800-171, incident reporting, and supplier flow-downs remain in force.

Updated September 24, 2026

The most expensive mistake the electronics channel can make right now is to read 'CMMC suspension' as 'cybersecurity suspension.' The July 13 order halted the upcoming Phase 2 transition and the use of new third-party and government-led certification requirements during the review. It did not cancel CMMC or remove existing contractual safeguarding requirements.



It did not erase DFARS 252.204-7012, NIST SP 800-171 Revision 2, required self-assessments, SPRS records, annual affirmations, 72-hour cyber incident reporting, or applicable supplier flow-downs. And it did not rewrite the cybersecurity terms that primes and Tier 1 customers place in their own agreements.

PAUSED The Phase 2 transition and new Level 2 C3PAO or Level 3 DIBCAC assessment requirements during the suspension.

STILL ACTIVE CMMC Level 1 and Level 2 self-assessments may still be required in solicitations and contracts.

UNCHANGED DFARS 252.204-7012, NIST SP 800-171 Rev. 2, 72-hour reporting, SPRS records, annual affirmations, and applicable flow-downs.

COMMERCIAL REALITY Prime contractors and Tier 1 customers can continue enforcing their own supplier cybersecurity terms.

For ECIA members, that distinction matters because cybersecurity requirements often arrive before a company thinks of itself as a defense contractor. A controlled drawing attached to an RFQ, a test report sent by email, or a portal export containing Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) can change the scope quickly.

The suspension is narrower than the headline

On July 13, 2026, the Department of War suspended the transition to CMMC Phase II, including the planned November 10, 2026 start of new third-party certification requirements. It also launched a 60-day review of compliance costs, assessment capacity, and barriers for smaller and non-traditional defense suppliers. That review period has passed. As of September 24, the Department has not published a replacement start date for Phase II or a public set of reform recommendations.

The Department has since carried the pause into contracting instructions. The September 3 revision of DFARS Class Deviation 2026-O0025 directs contracting officers to remove or revise affected assessment requirements in solicitations and contracts. During the suspension, requiring activities may still specify CMMC Level 1 or Level 2 self-assessments. They may not require new Level 2 C3PAO or Level 3 DIBCAC assessments under the suspended transition. Check the actual clause and any contract modification with your customer rather than assuming an existing purchase order changed automatically.

That is meaningful relief from the certification bottleneck. The Department's CMMC guidance still describes Phase I self-assessments as active, and existing safeguarding clauses continue to apply where incorporated into contracts. The September contracting revision implements the pause; it does not announce when third-party certification will resume.

The obligations that stayed put

- **DFARS 252.204-7012.** Covered defense information still must be safeguarded, and qualifying cyber incidents still must be reported within 72 hours. Other response and preservation duties in the clause remain relevant as well.
- **NIST SP 800-171 Rev. 2.** The 110 security requirements remain the baseline for systems that process, store, or transmit CUI under the applicable contract clauses.
- **FAR 52.204-21.** Basic safeguarding requirements for FCI still reach suppliers that may never handle CUI.
- **SPRS assessments and annual affirmations.** Required self-assessment results and affirmations of continuous compliance must remain accurate and current. A stale or optimistic record is not made safer by the pause.
- **Flow-down obligations.** When a subcontractor or supplier will process, store, or transmit FCI or CUI, the prime or higher-tier contractor must determine and communicate the applicable requirements before award and throughout performance.
- **Truthful representations.** The Justice Department continues to pursue False Claims Act matters involving alleged cybersecurity noncompliance. A delayed certification date does not reduce the risk of an inaccurate score, attestation, or customer response.

How a normal RFQ can widen your scope

Consider a common channel transaction. A manufacturers' representative receives an RFQ and forwards a controlled drawing to an authorized distributor and the component manufacturer. Within minutes, copies may exist in three mail systems, local download folders, a CRM record, a shared drive, mobile devices, and several backup platforms. The data moved before anyone asked whether it was FCI or CUI.

CMMC scope follows the information, the contract, and the systems used to handle it. It does not follow the company's marketing description. A distributor or rep firm does not avoid the issue simply because it is not the prime contractor.

Commercially available off-the-shelf (COTS) treatment can matter, and awards solely for COTS items are generally excluded from the CMMC clause. But a COTS part number is not a blanket answer. Controlled information exchanged around the transaction, non-COTS work, customer-specific services, and private contract language can create separate obligations. ITAR status is also a different legal question; one label should not be used as a shortcut for another.

Use the pause to make deliberate choices

- **Find the data before buying tools.** Trace FCI and CUI from intake through email, portals, endpoints, shared drives, PLM, ERP, CRM, backups, managed service providers, and disposal. The system boundary should reflect the real workflow.
- **Decide whether to accept CUI.** Some distributors and rep firms can keep controlled data in a customer or manufacturer portal, route it to a small compliant enclave, or decline to receive it. Make the choice deliberately and document it.
- **Keep the self-assessment honest.** Your SPRS record, system security plan, and plan of action and milestones should describe the environment that actually exists. Close old gaps and correct assumptions that no longer match operations.

- **Review customer answers before sales sends them.** Supplier questionnaires often blend CMMC, NIST, export control, privacy, and general security questions. Route answers through people who understand both the contract and the technical environment.
- **Continue the control work.** Multi-factor authentication, access control, FIPS-validated encryption where required, logging, incident response, vulnerability management, and a defensible cloud boundary protect the data regardless of how the assessment model changes.
- **Practice the 72-hour response.** A reportable incident can involve several suppliers and customers at once. Confirm who gathers evidence, who contacts the government, who notifies customers, and how records are preserved.

The review may change the mechanism, not the need

The 60-day review period has ended, but the Department has not publicly settled the next Phase II date or assessment model. The September contracting revision tells buyers how to administer the current pause. It does not resolve what will follow it. Members should watch for formal Department guidance and read each solicitation and flow-down clause on its own terms.

CMMC is a verification mechanism layered over longstanding contract requirements. The companies that use this period to narrow scope, correct their evidence, and finish the underlying work will be ready for the next policy. The companies that stop will restart under pressure while customer questionnaires and purchase-order clauses continue to arrive.

The next move belongs to the channel

The certification timetable is unsettled. The obligation to protect defense information remains. For manufacturers, authorized distributors, and manufacturers' representatives, the practical question is whether the company knows what information it receives, where that information goes, what it has promised customers, and whether those promises are true.

Join the ECIA cybersecurity conversation

The ECIA Global Industry Practices Committee's Cybersecurity Working Group is comparing how manufacturers, authorized distributors, manufacturers' representatives, and service providers are handling CMMC scoping, customer questionnaires, flow-down language, and practical control implementation. Contracts, compliance, operations, IT, and cybersecurity professionals all have useful experience to contribute. Participation is open to ECIA members and non-members.

To participate, contact Stephannie Bronson at sbronson@ecianow.org or visit the [Global Industry Practices Committee page](#).

Sources and further reading

- [Department of War CIO: CMMC program page and Phase II suspension notice](#)
- [Department of War CIO: Removing Barriers to DIB Expansion memorandum](#)
- [Department of War CIO: Implementing Suspension of CMMC Phase II](#)
- Defense Acquisition Regulations System: DFARS Class Deviation 2026-O0025, Revision 3 (September 2026)
- [Acquisition.gov: DFARS 252.204-7021](#)
- [Federal Register: CMMC contractual implementation final rule](#)
- [U.S. Department of Justice: 2026 False Claims Act cybersecurity enforcement example](#)
- [ECIA: Global Industry Practices Committee](#)

This article provides general information, not legal advice. Scope and obligations depend on the product, entity, contract, data, and applicable national law.