DTS IT ADVISORS | CMMC MANUFACTURER BRIEF

CMMC After the Phase II Pause: What Manufacturers Still Need to Do

A practical guide to contracts, CUI, scope, evidence, spending, and provider selection

By Henry Decoo, Founder & Senior Technology Advisor, DTS IT Advisors

Based on an August 26, 2026 SAMA webinar discussion with Sean Burke of Ariento. Updated against official guidance as of August 27, 2026.

BOTTOM LINE

The Phase II pause created more time to make good decisions. It did not remove the need to understand your contracts, protect sensitive information, or support what your company affirms.

Manufacturers in the defense supply chain are asking a reasonable question: if Phase II of CMMC was paused, should we keep preparing? The answer is yes, but preparation should be disciplined. The immediate priorities are to clarify obligations, identify CUI, control scope, build evidence, and avoid buying tools before the business problem is defined.

The pause changed the timeline, not the need for cybersecurity

On July 13, 2026, the Department of War suspended the transition to Phase II of CMMC and other pending implementation milestones while it reviews the program. That change matters, but it does not mean manufacturers can ignore cybersecurity requirements already tied to their work.

The Department says Phase I self-assessment requirements remain in place. Level 1 addresses Federal Contract Information, or FCI, through 15 basic safeguarding requirements. Level 2 addresses Controlled Unclassified Information, or CUI, through 110 requirements drawn from NIST SP 800-171 Revision 2. Under the current Phase I framework, Level 2 self-assessments are conducted every three years and an authorized company official affirms continued compliance annually.

The practical business takeaway from our webinar was simple: a delayed deadline does not erase a signed contract. Manufacturers still need to understand what their contracts require, what information they handle, and what their customers or prime contractors expect.

Start with the contract, not the acronym

CMMC conversations often start with labels such as Level 1, Level 2, RPO, C3PAO, or FedRAMP. A manufacturer should start one step earlier. Review the actual contract, solicitation, purchase order, and subcontract flow-down language.

A prime contractor can impose requirements through its subcontracting process, and it may consider cybersecurity readiness when evaluating supplier risk. If the language is vague, ask the prime or contracting contact to clarify the required CMMC status, applicable DFARS clauses, the expected handling of CUI, and the timing. Document the answer rather than relying on an informal assumption.

This is not just a compliance exercise. A supplier that cannot accept protected information when a program needs it may create schedule and sourcing risk for the prime. That can affect competitiveness even while broader certification milestones are under review.

Determine whether you actually handle CUI

CUI is not simply any information related to a government customer. It is unclassified information that falls within an approved CUI category and requires safeguarding or dissemination controls under law, regulation, or government-wide policy. Contracts and agency guidance determine how those requirements apply to industry.

For a manufacturer, likely examples can include controlled technical information, certain engineering drawings, specifications, test information, or derivative files created while performing the work. A public specification, ordinary shipping record, or routine purchase order is not automatically CUI.

Do not make this determination from file names alone. Review markings, contract requirements, the CUI category involved, and guidance from the prime or contracting activity. Contractors may also create CUI on behalf of the government when their agreement authorizes or requires it. If the status of information is unclear, obtain a written answer before deciding that it is inside or outside your protected environment.

Scope drives both risk and cost

Once CUI is identified, trace one realistic job from receipt through final disposition. Follow the drawing or data through email, customer portals, engineering workstations, file servers, cloud applications, backups, printers, CNC workflows, mobile devices, remote users, and downstream suppliers.

Every person, device, system, location, and service provider that processes, stores, transmits, or protects that information can affect the assessment scope. A missing asset creates risk. An unnecessarily broad boundary increases licensing, remediation, monitoring, documentation, and assessment costs.

This is why buying software before mapping the workflow is so often wasteful. The manufacturer should first document the current data flow, define the intended protected boundary, identify dependencies, and record why each asset is in or out of scope.

An enclave is a scope strategy, not an automatic shortcut

An enclave is a separated environment designed to keep CUI within a controlled boundary. It can make sense when a limited group of people performs a limited set of sensitive tasks and can work effectively inside that boundary.

It may be a poor fit when CUI must move continuously through engineering, shop-floor systems, printers, cloud applications, multiple locations, or outside suppliers. The operational question is not simply whether an enclave is available. It is whether employees can complete the required work without repeatedly moving information outside the boundary.

Manufacturers should compare a self-managed enclave, a managed enclave, and a broader enterprise approach based on workflow, responsibility, flexibility, ongoing cost, and assessment scope. A provider should document which controls it operates, which responsibilities remain with the manufacturer, what endpoints and users remain in scope, and what activities are restricted.

Policies are not proof

A written policy describes what should happen. Readiness depends on whether the process is implemented, followed, monitored, and supported by evidence. That evidence may include configurations, access records, training records, incident procedures, risk reviews, inventories, logs, tickets, and other artifacts tied to the assessment objectives.

Management owns more than the budget. Leadership must approve the scope, assign responsibility, support changes to business processes, and make any required affirmation based on an accurate picture of the environment. Internal IT and outside providers can implement controls, but the manufacturer cannot assume that an MSP automatically owns every CMMC responsibility.

A shared responsibility matrix is a practical way to show who implements, operates, documents, and provides evidence for each requirement. If responsibility is not written down, it is likely to become a gap later.

Spend money in the right sequence

The goal is not to find the cheapest path. It is to avoid paying for the wrong solution before the problem is understood. A sensible sequence is:

- Verify contract requirements, information types, customer expectations, and internal ownership.
- Map how FCI and CUI enter, move through, and leave the business.
- Define and document the assessment scope and intended operating workflow.
- Assess the controls and evidence that are actually in place.
- Prioritize remediation by risk, contractual need, operational impact, and dependency.
- Select technology and service providers only after the required outcomes are clear.

Common premature purchases include broad government-cloud licensing, duplicate hardware, evidence-gathering platforms, and enclave services that do not fit the production workflow. Each can be valuable in the right design. None should substitute for scope and workflow analysis.

Match each provider to the job

Manufacturers often receive proposals that look similar but solve different problems. A managed service provider, or MSP, may run day-to-day technology and implement controls. A managed security service provider, or MSSP, focuses on monitoring, detection, and response. A CMMC consultant or Registered Practitioner Organization may help interpret requirements, define scope, identify gaps, and prepare. A C3PAO performs authorized Level 2 certification assessments when that assessment is required.

Before signing, ask the provider to define the systems, users, locations, services, and subcontractors included in the engagement. Confirm assumptions, exclusions, work products, acceptance criteria, remediation support, licensing, implementation charges, recurring fees, travel, retesting, contract term, data ownership, and offboarding.

Also ask how assessment independence and conflicts of interest will be handled. Preparation and certification are different roles. The proposal should clearly show who is advising, who is implementing, who may assess, and who remains responsible after the initial project is complete.

A practical 30-60-90 day plan

- First 30 days: collect contracts and flow-down clauses, identify likely FCI and CUI, name an executive owner, and map the current information flow.
- By 60 days: validate the scope, complete or refresh the assessment, identify high-risk gaps, and document provider responsibilities.
- By 90 days: remediate priority gaps, test whether employees follow the intended workflow, collect evidence, and confirm that management can support any required submission or affirmation.

Companies already in progress should not automatically move to the next purchase. They should first confirm that the scope, assumptions, and evidence still match the way the business actually operates.

The four decisions to make now

- Confirm what your contracts and customers require.
- Determine whether you receive or create CUI.
- Validate the people, systems, locations, and providers inside the scope.
- Choose the next investment only after the required outcome is defined.

INDEPENDENT NEXT STEP

If you are unsure whether you handle CUI, whether your scope is too broad, or whether two proposals are truly comparable, schedule an independent CMMC readiness discussion before committing to a major solution.

Henry Decoo | Founder & Senior Technology Advisor

941-559-8028 | hdecoo@dtsitadvisors.com | Schedule a discussion

Official sources

- Department of War, CMMC program page and Phase II suspension update
- Department of War, About CMMC
- Department of War, Implementing Suspension of CMMC Phase II
- Electronic Code of Federal Regulations, 32 CFR Part 170
- National Archives, Controlled Unclassified Information Registry