



CMMC Has Changed Your Cybersecurity Requirements Have Not

If your company supports the Department of Defense or supplies a prime contractor, protecting Controlled Unclassified Information (CUI) remains a contract requirement. While the Department has temporarily paused mandatory third-party CMMC Level 2 certification requirements during its program review, organizations handling CUI are still expected to comply with NIST SP 800-171 and complete applicable self-assessments. Manufacturers that prepare now will be better positioned for future contract opportunities while avoiding unnecessary cost and disruption.

What Changed?

Previous Expectation

Third-party Level 2 audits were expected to expand under Phase II.

Many companies felt pressure to rush toward certification.

Many planned enterprise-wide compliance projects.

Current Reality

Mandatory Phase II third-party audits are temporarily suspended while the program is reviewed.

Organizations should continue preparing for Level 2 self-assessments and protecting CUI.

Many manufacturers can reduce costs through proper scoping and enclave strategies.

What manufacturers should do now

- 1. Confirm applicability.** Identify whether you handle FCI only, CUI, ITAR/export-controlled data, or prime-contractor flowdowns.
- 2. Scope before you spend.** Decide whether all systems are in scope or whether a smaller enclave is appropriate.
- 3. Run a readiness assessment.** Compare your current environment to NIST SP 800-171 Level 2 requirements and document gaps.
- 4. Build the remediation plan.** Prioritize the items that block certification, including MFA, logging, access control, asset inventory, policies, and evidence collection.
- 5. Build a roadmap.** One that supports today's self-assessment requirements while remaining ready for future certification.

A Smarter Approach for Many Manufacturers

Not every company needs to secure its entire environment. Many manufacturers can significantly reduce cost, implementation time, and operational disruption by limiting the users and systems that handle CUI through a properly designed enclave strategy.

A readiness assessment helps determine:

- Whether an enclave is appropriate
- Which users actually require CUI access
- Which systems can remain out of scope
- The most cost-effective path to compliance

Before investing in CMMC, make sure you're solving the right problem. We help manufacturers evaluate their contracts, identify their CUI footprint, and determine whether an enterprise implementation, enclave strategy, or another compliance approach best fits their business.

Contact Us

Allison Evanitz, Business Advisor: allison.evanitz@floridamakes.com

Rob Harris, Executive Director: execdir@sama-fl.com