
BLACKTECHSTARTUP EDUCATION

CMMC Is a Sales Gate: Build the Evidence the Current Rules Still Require

CMMC changed again in July 2026. Phase II requirements were suspended while Phase I self-assessment requirements remain. Small tech contractors still need disciplined evidence around FCI, CUI and NIST controls if they want defense work.

CMMC changed again in July 2026. Phase II requirements were suspended while Phase I self-assessment requirements remain. Small tech contractors still need disciplined evidence around FCI, CUI and NIST controls if they want defense work.

Start with the rule that exists today

As of August 17, 2026, the Department of War's CMMC program page says Phase II requirements were suspended on July 13, 2026 while the Department reviews and reforms implementation. It also says Phase I self-assessment requirements remain in place. That means a small contractor should not build its plan around an outdated rollout chart or assume CMMC disappeared. Contract language, the information you handle and current solicitation requirements still control. Treat every opportunity as a fresh applicability check and save the official requirement that supports your decision.

Know whether the work touches FCI or CUI

Federal Contract Information and Controlled Unclassified Information are not interchangeable. Before quoting a project, ask what data will enter your systems, where it will be stored, who will access it, whether subcontractors will touch it and what clauses are in the contract. Draw the system boundary. A company can create unnecessary compliance burden by casually allowing sensitive project data into every laptop, SaaS tool and personal device. Conversely, under-scoping the environment can leave evidence gaps. The commercial move is to design the smallest defensible environment that supports the work.

Build evidence as you implement controls

A control that exists only in someone's memory is hard to defend. Create an evidence repository with policies, system diagrams, asset inventories, access lists, configuration standards, training records, incident procedures, screenshots or exports where appropriate, and records of periodic reviews. Keep dates and owners. For NIST SP 800-171 practices relevant to CUI, understand what the requirement means operationally and what evidence demonstrates performance. Documentation should reflect the real environment; copied policy templates that describe controls you do not operate create risk rather than reducing it.

Treat subcontractors and cloud vendors as part of the sales decision

If a subcontractor processes project information or a cloud service stores regulated data, their capability affects yours. Ask vendors what environment, authorization, encryption, logging, incident support and data-location commitments they provide. Map data flows before onboarding a new SaaS product because 'we use Microsoft' or 'we use AWS' is not itself a compliance answer. If you are the prime contractor, define what evidence you need from subs. If you are a sub, be ready to explain your boundary and responsibilities clearly to the prime.

Turn security readiness into procurement speed

The revenue advantage is not a badge; it is being able to answer security questions quickly and credibly. Keep a capability packet containing your system boundary, control responsibility matrix, incident contact, current assessment status and approved tools. When a buyer asks whether a project can operate in your environment, you can respond in hours rather than launching a six-week scramble. That can matter for Black-owned small firms competing against larger incumbents because speed and clarity lower the buyer's perceived execution risk.

The current-state action plan

First, read the official CMMC page and the specific solicitation or contract clauses for the opportunity in front of you. Second, classify the information flow and draw the environment boundary. Third, assess the applicable NIST SP 800-171 requirements and preserve evidence of what is implemented. Fourth, identify gaps with owners and dates rather than hiding them. Fifth, review vendor and subcontractor data flows. Finally, schedule a monthly rules check because the Department has explicitly said the program is under review. Do not let a consultant's old slide deck become your source of truth.

The defense-buyer readiness packet

Keep a concise packet ready for primes and contracting teams, but only include claims you can support. Page one: company and point of contact, contract identifiers where applicable, services, and the types of federal information your approved environment is designed to handle. Page two: system boundary diagram showing users, endpoints, cloud services and external connections. Page three: control-responsibility map identifying which safeguards are company-operated and which depend on a cloud or managed provider. Page four: current self-assessment status and dates, with sensitive details shared only through appropriate channels. Page five: incident-reporting contacts, approved file-transfer methods and subcontractor rules. Maintain an evidence index behind the packet rather than sending configuration screenshots indiscriminately. Review the packet every quarter and after material environment changes. Because CMMC is in active reform in 2026, add a 'requirements checked' date and link the official DoW source used. This packet turns security from a late proposal scramble into sales enablement. It also protects the firm from an employee casually promising a certification, authorization or data-handling capability the company does not have. Accuracy is part of credibility.

Do not confuse readiness with certification

Use precise language in proposals. Say what assessment or control work has actually been completed and what requirement the solicitation states. Do not advertise 'CMMC certified' unless the company holds the applicable current credential and can substantiate it. During a changing program, accuracy protects credibility with primes and contracting officers.

Research behind this guide

Use the primary sources below to verify current rules, eligibility and program details before acting. Program terms can change.

Department of War CIO — Cybersecurity Maturity Model Certification



Department of War CIO — About CMMC



Department of War CIO — CMMC resources and documentation



NIST — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations



Important: This article is educational information, not individualized legal, tax, investment or compliance advice. For decisions with legal or financial consequences, use a qualified professional who can review your facts.

SHARE THIS GUIDE ↗

POWERED BY: BLACK TECH STARTUP

blacktechstartup.com