DEFENSE READINESS • SEP 23, 2026 • 7 MIN READ

CMMC for a 20-Person Shop: What Actually Applies to You

Most small suppliers don't need a six-figure compliance program. They need to know which level applies, what's actually in force today, and where to start.

If you machine parts, provide services, or subcontract to a defense prime, someone has probably told you that **CMMC** (the Cybersecurity Maturity Model Certification) is coming for you. Some of them were selling something. The honest answer for a 20-person shop is: it depends on what information touches your business, and it's probably smaller than you've been told.

First question: what information do you handle?

CMMC is built around two kinds of information:

- **Federal Contract Information (FCI).** Non-public information provided by or generated for the government under a contract. Nearly every defense supplier handles some.
- **Controlled Unclassified Information (CUI).** Information the government requires you to safeguard, often technical drawings, specifications and data that carry distribution or export markings. If your prime sends you marked drawings, assume CUI until someone tells you otherwise in writing.

Which of these lands in your inbox, your file server or your shop-floor terminals decides everything that follows.

Level 1 or Level 2?

- **Level 1: FCI only.** Fifteen basic safeguarding requirements from FAR 52.204-21: things like limiting who can log in, using passwords, keeping malware protection current and controlling

physical access. You self-assess every year and a senior official affirms the result in the Supplier Performance Risk System (SPRS).

- **Level 2: you handle CUI.** The 110 requirements of NIST SP 800-171 Revision 2, across 14 families. Depending on the contract, it's a self-assessment or an assessment by an accredited third party (a C3PAO).
- **Level 3** covers a small number of the most sensitive programs. A 20-person shop is unlikely to see it.

Where the rollout stands (September 2026)

The DFARS rule that puts CMMC into defense contracts took effect on **10 November 2025**. That opened Phase 1: new solicitations can require a Level 1 or Level 2 self-assessment as a condition of award.

Phase 2 would have made third-party Level 2 certification a condition of award for many CUI contracts starting 10 November 2026. In **July 2026 the Department suspended Phase 2** and the later milestones while it reviews the program. As of this writing, no new date has been set.

Don't read the pause as a reprieve. Self-assessment requirements are live in new contracts. DFARS 252.204-7012, which requires safeguarding CUI and reporting cyber incidents, has been in contracts with CUI for years. And if someone at your company has affirmed compliance in SPRS, that affirmation needs to be true.

> *The pause changed the date on the certificate. It didn't change what's already in your contract.*

How to start without overbuying

1. **Read your contracts, then ask your prime.** Look for FAR 52.204-21 and DFARS 252.204-7012, -7019, -7020 and -7021. Ask in writing whether you receive CUI, and which CMMC level they expect.
2. **Scope before you secure.** Find where FCI and CUI actually live. Shrinking that boundary (one enclave, a few machines, a few people) is usually the single biggest cost saver.

3. **Run an honest gap assessment** against the right list: 15 requirements or 110. Mark each one met, partly met or not met, with the evidence.
4. **Write the system security plan to match reality.** Describe what your shop really does, not what a template says you do.
5. **Fix in order of risk.** Multi-factor authentication, account and access control, patching, backups and logging close most of the real exposure early.
6. **Keep evidence as you go.** Screenshots, configs and sign-offs gathered while you work are cheap. Reconstructing them the week before an assessment is not.

Where AI fits, and where it doesn't

AI is genuinely useful here: drafting policies from your real practices, organizing evidence, summarizing logs, and turning a 110-line spreadsheet into a work plan. It removes a lot of the paperwork that makes small shops give up.

The hard line: **CUI does not go into a consumer AI tool.** Only use AI inside environments that meet the requirements for handling it. When the answer is no, the right move is to keep that work manual, not to find a workaround.

This is a field report, not legal advice. The program is changing. Check the DoD CIO CMMC page and your own contract language before you act.

Nick Vandam — founder of Contact Creek. West Point graduate, veteran U.S. Army officer, small-business owner and Thunderbird-trained. Writes about defense readiness and where technology actually earns its keep in a working business.

The Library · info@contactcreek.com