CMMC Level 1: what still applies

A one-page guide for small defense contractors · October 2026

FEDERALSHIELD

Does it apply to you? If you hold a DoD contract or subcontract and handle Federal Contract Information (FCI), meaning information the government gives you or you produce for it that isn't meant to be public, then FAR 52.204-21 applies, and so does CMMC Level 1 when your solicitation calls for it.

"Isn't CMMC paused?" Only Phase 2, which covers third-party (C3PAO) assessments for many Level 2 contracts and was suspended in July 2026. Phase 1 stays in force: the Level 1 self-assessment and the **annual affirmation in SPRS**, signed by a senior company official.

The 15 requirements (FAR 52.204-21), in plain English

1. **Authorized users only**
   Only approved people, programs and devices can use your systems.
2. **Right access for each role**
   People can only do what their job needs.
3. **Control outside systems**
   Know and limit connections to systems you don't control, such as personal devices and outside cloud accounts.
4. **Watch what goes public**
   Review anything posted to public websites so FCI isn't exposed.
5. **Identify users and devices**
   Everyone gets their own login, with no shared accounts.
6. **Verify before access**
   Use passwords, and ideally multi-factor sign-in.
7. **Wipe or destroy old media**
   Clean or shred drives and paper before disposal or reuse.
8. **Limit physical access**
   Lock offices, server closets and equipment.
9. **Manage visitors and keys**
   Escort visitors, keep a visitor log, and track keys and badges.
10. **Separate public systems**
    Keep anything public-facing, such as a website or guest Wi-Fi, apart from your internal network.
11. **Protect the network edge**
    Use a firewall to monitor and control traffic in and out.
12. **Fix flaws promptly**
    Turn on automatic updates and patch known issues.
13. **Malware protection**
    Run antivirus or endpoint protection on your systems.
14. **Keep it updated**
    Make sure malware protection updates itself.
15. **Scan regularly**
    Run periodic scans and scan files from outside sources, such as downloads, email and USB drives, when they're opened.

Four steps, once a year

1. Assess
Check each requirement and note your evidence: a screenshot, a policy or a log.

2. Fix
Close every gap. Level 1 is pass/fail, and plans of action (POA&Ms) aren't allowed.

3. Enter in SPRS
Record your self-assessment result in the Supplier Performance Risk System.

4. Affirm
A senior official affirms compliance in SPRS, and the affirmation is repeated every year.

Free resources

Plain-English guide: what the Phase 2 pause does and doesn't change, with a 30-day plan.
federalshield.tech/blog

Free Level 1 self-assessment: walk through all 15 requirements online and see your gaps.
app.federalshield.tech

FederalShield Cybersecurity LLC · 50 W Broadway #300, Salt Lake City, UT 84101 · +1 385 379 6200 · federalshield.tech

General information, not legal advice. FederalShield is not affiliated with or endorsed by the Department of War (DoD).