AETOS ONE

MANAGED SECURITY OPERATIONS

CMMC Level 1 Compliance: The Path of Least Resistance

A practical guide for DIB subcontractors on meeting FAR 52.204-21 with maximum protection and minimum cost

AETOS ONE | WHITE PAPER | 2026

CONTENTS

Table of Contents

Executive Summary

If your company touches Federal Contract Information (FCI) on a Department of Defense contract, CMMC Level 1 applies to you. The requirement isn't new. It's been in place since 2016 under FAR clause 52.204-21. What's new is verification: you must now **self-assess** against 15 basic safeguarding requirements, **submit the results** to the Supplier Performance Risk System (SPRS), and **affirm compliance** every year.

This paper explains what Level 1 requires, what it doesn't require, and how to reach a Final Level 1 (Self) status without overbuilding your security program. Level 1 is the floor, not the ceiling. Contractors who treat it as a ceiling waste money on controls the rule does not ask for. Contractors who treat it as a floor position themselves for Level 2 work later, at a lower incremental cost.

You have the option to build Level 1 compliance internally, or to maintain it through a CMMC-trained managed security services provider (MSSP). For most subcontractors under roughly 50 employees, the numbers favor the MSSP path, and the reasons go beyond cost.

1. What CMMC Level 1 Really Requires

CMMC Level 1 protects **Federal Contract Information** (FCI): information the government provides or generates under a contract, not intended for public release, excluding simple transactional data like payment processing. It doesn't cover **Controlled Unclassified Information** (CUI). If your contracts involve CUI, you need Level 2, which is a separate and larger undertaking.

Level 1 consists of exactly 15 requirements, taken word for word from FAR clause 52.204-21(b)(1)(i) through (xv). CMMC adds no new requirements at Level 1. The Level 1 Self-Assessment Guide confirms this directly: the guide "can be used as part of preparation for and conducting a Level 1 self-assessment," and the requirements trace to NIST SP 800-171A objectives for scoring purposes only.

The 15 requirements, mapped to 6 control families

Each requirement below is assessed as MET or NOT MET. There is no partial credit and no Plan of Action and Milestones (POA&M) at Level 1. **Every requirement must be MET** to achieve Final Level 1 (Self) status.

This table is the same structure used in Aetos One's Level 1 self-assessment tool (https://aetosone.com/cmmc/cmmc-l1-assessment.html), which walks each requirement through Examine, Interview, and Test objectives drawn from NIST SP 800-171A, so your team sees exactly what an assessor would look for before you submit to SPRS.

ID	REQUIREMENT	FAM.
AC.L1-b.1.i	Limit system access to authorized users, processes, and devices.	AC
AC.L1-b.1.ii	Limit access to the types of transactions and functions authorized users may execute.	AC
AC.L1-b.1.iii	Verify and control or limit connections to external information systems.	AC
AC.L1-b.1.iv	Control information posted or processed on publicly accessible systems.	AC
IA.L1-b.1.v	Identify system users, processes acting on behalf of users, or devices.	IA
IA.L1-b.1.vi	Authenticate or verify identities before allowing access.	IA
MP.L1-b.1.vii	Sanitize or destroy media containing FCI before disposal or reuse.	MP
PE.L1-b.1.viii	Limit physical access to systems, equipment, and operating environments to authorized individuals.	PE
PE.L1-b.1.ix	Escort visitors, monitor visitor activity, maintain physical access logs, and control physical access devices.	PE
SC.L1-b.1.x	Monitor, control, and protect communications at external and key internal boundaries.	SC
SC.L1-b.1.xi	Implement subnetworks for publicly accessible components, separated from internal networks.	SC
SI.L1-b.1.xii	Identify, report, and correct information and system flaws in a timely manner.	SI
SI.L1-b.1.xiii	Provide protection from malicious code at appropriate locations.	SI
SI.L1-b.1.xiv	Update malicious code protection when new releases are available.	SI
SI.L1-b.1.xv	Perform periodic scans and real-time scans of files from external sources.	SI

AC = Access Control | IA = Identification & Authentication | MP = Media Protection | PE = Physical Protection | SC = System & Communications Protection | SI = System & Information Integrity

Source: FAR clause 52.204-21(b)(1)(i)-(xv), as mapped to CMMC Level 1 security requirements in 32 CFR § 170.14(c)(2) and Table 2 to § 170.15(c)(1)(ii).

15 of 15

Every requirement must be MET. No partial credit, no Plan of Action and Milestones, at Level 1.

2. Keep Your Scope Small on Purpose

The single biggest cost lever at Level 1 is scope. Under 32 CFR § 170.19(b), **only assets that process, store, or transmit FCI are in scope**. Everything else is out of scope, with no documentation burden at all.

Three asset categories matter:

- **In-scope assets.** Any system that processes, stores, or transmits FCI. These get assessed against all 15 requirements.
- **Out-of-scope assets.** Systems that never touch FCI. A workstation with no FCI exposure carries zero Level 1 obligation. A properly configured VDI client, where only keyboard, video, and mouse signals pass through, is also out of scope.
- **Specialized assets.** IoT devices, OT, government-furnished equipment, restricted systems, and test equipment that can touch FCI but cannot be fully secured. These are excluded from the Level 1 assessment scope entirely.

In short, if your FCI work happens on three laptops and one file share used by two employees, your assessment scope is those four assets, not your entire network. Isolate the FCI workflow into a small, well-defined enclave, and you shrink both the assessment effort and the ongoing burden of the annual affirmation.

Scoping guidance recommends inventorying the people, technology, facilities, and external service providers that touch FCI before you assess anything. That inventory is 30 minutes of work that can save weeks of unnecessary control implementation on systems that were never in scope to begin with.

3. Low-Cost, High-Leverage Paths to Each Control Family

None of the 15 requirements demand enterprise tooling. Most are achievable with configuration changes and documented practices using what a small business already owns.

Access Control and Identification & Authentication

Use named user accounts, never shared logins. This alone satisfies the identification objective for AC.L1-b.1.i and IA.L1-b.1.v.

Turn on multi-factor authentication on email and any cloud application touching FCI. Microsoft 365 Business Premium and Google Workspace both include this at no extra licensing cost.

Disable guest network access to any segment where FCI-handling devices live, or place FCI devices on a separate VLAN from guest Wi-Fi.

Media Protection

Use built-in OS tools (Windows "cipher /w" or a certified wipe utility) before retiring or reselling any device that stored FCI. Document the date and method.

Physical Protection

A locked door and a visitor sign-in sheet satisfy PE.L1-b.1.viii and PE.L1-b.1.ix for most small offices. No badge system is required by the rule.

System & Communications Protection

A consumer or small-business firewall with default-deny inbound rules satisfies the boundary protection objective in SC.L1-b.1.x for most environments this size.

If you host a public website, **keep it on separate infrastructure** from any system that touches FCI. That satisfies SC.L1-b.1.xi without a physical subnetwork build-out.

System & Information Integrity

Enable automatic OS and application patching. This satisfies the timely-correction objective in SI.L1-b.1.xii for most small environments.

Built-in endpoint protection (Microsoft Defender, included free with Windows) with automatic definition updates and scheduled scans satisfies SI.L1-b.1.xiii through SI.L1-b.1.xv without a separate antivirus purchase.

The pattern across all 15 requirements holds true: configure what you already have correctly, document what you did, and keep the FCI footprint small. That combination clears Level 1 for the large majority of subcontractors without new capital spend.

4. The Part Companies Underestimate: Annual Affirmation

Achieving Final Level 1 (Self) status is a point-in-time event. Staying compliant is not. Under 32 CFR § 170.15(a)(1) and § 170.22, an Affirming Official, a senior representative of your company, **must submit a new affirmation to SPRS every year** attesting that all 15 requirements remain MET.

Three details matter here and are frequently missed:

- **No POA&Ms are permitted at Level 1**. Every requirement must be MET at the time of assessment. There is no partial-credit path like there is at Level 2.
- **A new assessment, not just a new affirmation, is required if your CMMC Assessment Scope changes materially** (for example, a network expansion, a merger, or a new location handling FCI).
- **Assessment artifacts must be retained for six years from the CMMC Status Date**, even though Level 1 itself has no formal documentation requirement to create those artifacts in the first place.

This is where most subcontractors lose ground. The initial assessment gets attention because a contract deadline forces it. The next year's affirmation does not have the same forcing function, and configurations drift: a firewall rule gets changed for a project and never reverted, a new laptop joins the network without MFA enrolled, an employee leaves and their account stays active. None of this shows up until the affirmation is due, or worse, until a prime contractor or DoD audit asks for evidence you no longer have.

5. Build Internally or Maintain Through an MSSP

The Department of Defense's own CMMC rulemaking includes cost estimates for a small entity to complete a Level 1 self-assessment and initial affirmation: roughly $5,977 in the first year, based on a director and an external IT specialist working through planning, assessment, and SPRS reporting, plus an estimated $560 for each annual reaffirmation after that.

$5,977

DoD estimate for a small entity's first-year Level 1 self-assessment and initial affirmation.

$560/yr

DoD estimate for each annual reaffirmation after year one, assuming no drift or gaps.

That estimate assumes the basic safeguarding requirements are already implemented, which is the DoD's own baseline assumption for every Level 1 contractor since the requirements have been contractually mandated since 2016. In practice, most small subcontractors have gaps: MFA not fully enrolled, no documented media sanitization process, no visitor log, patching not automated. Closing those gaps is where the real cost lives, and it is recurring, not one-time, because configurations drift and staff turn over.

Illustrative annual cost comparison

COST DRIVER	BUILD INTERNALLY (SMALL ENTITY)
Initial assessment & affirmation	~$5,977 (DoD estimate: director + ESP labor across planning, assessment, and SPRS reporting)
Annual reaffirmation	~$560/year per DoD estimate, assuming no drift or gaps found
Closing configuration gaps (MFA, patching, media sanitization, visitor logs)	Variable; typically the largest hidden cost, billed as ad hoc IT project work
Staying current on rule changes (32 CFR Part 170, SPRS process updates)	Owner or IT lead's time, opportunity cost against billable or operational work
Named security leadership	Not typically present at this size
Approximate monthly cost	**Variable, often underestimated until an audit or contract review exposes gaps**

Internal cost figures are DoD estimates from the CMMC Program final rule (32 CFR Part 170), Regulatory Impact Analysis, Small Entity cost tables. Actual internal cost varies by existing control maturity and is frequently higher once gap remediation is included. Aetos One pricing reflects the Guardian tier as published in current service tier documentation.

The comparison isn't simply cost per hour. **A director spending 12 hours a year on Level 1 paperwork is a director not spending those 12 hours running the business**. A CMMC-trained MSSP brings the requirement fluency to do the assessment correctly the first time, catches configuration drift before the annual affirmation is due, and carries institutional memory of your scope and evidence from one year to the next. That continuity is what most internal owners lose when the person who did last year's assessment changes roles or leaves the company.

220,000+

Companies in the Defense Industrial Base process, store, or transmit FCI or CUI in support of DoD programs, most without a dedicated security function.

This matters more than it might first appear. The DoD's own rulemaking record acknowledges the disproportionate burden this places on smaller entities relative to primes with in-house security teams. An MSSP exists to absorb exactly that burden at a predictable, fixed monthly cost instead of a variable, often underestimated internal one.

6. A Practical 30-Day Path to Level 1

WEEK 1	Inventory every asset, person, and external service provider that touches FCI. Draw the boundary tight.
WEEK 1	Confirm out-of-scope and specialized assets and exclude them in writing, even though documentation is not required. Future you will want the record.
WEEK 2	Run the 15 requirements against your in-scope assets using a structured tool. Mark each MET or NOT MET with the Examine, Interview, or Test evidence behind it.
WEEK 3	Remediate every NOT MET finding. Remember, POA&Ms are not permitted at Level 1. Everything must be MET before you submit.
WEEK 4	Submit your compliance result, CMMC Level, CMMC Status Date, Assessment Scope, and CAGE code(s) to SPRS. Have your Affirming Official submit the affirmation.
ONGOING	Calendar the annual reaffirmation date now, and assign an owner for configuration drift checks between now and then.

7. Staying Certified Is the Mandate

Getting to Final Level 1 (Self) status is the milestone every subcontractor is focused on today because a contract deadline demands it. But the CMMC rule was written around continuing compliance, not a single point-in-time event. Annual affirmation, artifact retention for six years, and a new assessment requirement the moment your scope changes all assume you are managing this as an ongoing program, not a one-time project.

A NOTE ON WHAT COMES NEXT

Getting certified is the milestone, but staying certified is the mandate.

Ask us how Citadel from Aetos One keeps your affirmation current, your evidence audit-ready, and your scope clean for the annual cycle, so the next assessment is a formality, not a fire drill.

cmmc@aetos.one | aetos.one