

ResilientTech Advisors

September 2025

CMMC Explainer

HOW DOD SUBCONTRACTORS & SUPPLIERS ARE
STAYING IN THE GAME

Why CMMC matters now

CMMC (Cybersecurity Maturity Model Certification) is the U.S. DoD's way of enforcing cybersecurity across its entire supply chain.

CMMC covers two types of **sensitive data**:

- 1. Federal Contract Information (FCI)**
- 2. Controlled Unclassified Information (CUI)**

Level	Applies To	Based On	Assessment
1 – Foundational	FCI	FAR 52.204-21 (17 practices)	Annual self-assessment
2 – Advanced	CUI	NIST SP 800-171 (110 controls)	3 rd party <i>or</i> self-assessment (contract dependent)
3 – Expert (future)	Highly sensitive CUI	NIST SP 800-172	Government-led

Who Is Affected

- Defense contractors & direct suppliers
- Tech providers supporting DoD work (IT, MSPs, Cloud/SaaS)
- Commercial firms handling FCI/CUI
- Independent consultants & niche vendors seeking direct DoD contracts

Impact: **220K** DIB entities^{1, 2}

1: DIB – Defense Industrial Base

2: Federal Register – CMMC Final Rule

CMMC Matters

Now



Planned Timeline

Dec 2024¹
Final Rule

Phased Implementation
2025-2027

Required & Enforced
2027

1: Federal Register – CMMC Final Rule

2: The [Office of Information & Regulatory Affairs \(OIRA\)](#) has 90 days to review CFR rules.

3: The “48 CFR rule” refers to the DoD acquisition rule that amends Title 48 of the Code of Federal Regulations to embed CMMC requirements into the Defense Federal Acquisition Regulation Supplement (DFARS).

Real Time Events

Oct 15, 2024 / Dec 16, 2024

Program rule published & effective
(32 CFR Part 170)

Jul 22, 2025

48 CFR rule submitted to OIRA for review

Sep 10, 2025²

48 CFR rule published; Phase 1 begins
with Level 1 & 2 self-assessments^{3, 4}

2026

Phase 2: Level 2 certification (C3PAO) for
applicable contracts⁵

2027

Phase 3: Level 3 certification (DIBCAC)
begins⁶

2028

Phase 4: Full implementation across all
applicable DoD contracts⁷

To make CMMC a contractual obligation, the DoD must amend the Defense Federal Acquisition Regulation Supplement (DFARS).

The Office of Information and Regulatory Affairs (OIRA) completed the 48 CFR rule review on September 25, 2025. This rule contains the DFARS amendments needed to enforce CMMC.

Now that the DFARS amendments have been published in the Federal Register, contracting officers can insert the new DFARS clause 252.204-7021 into solicitations, making CMMC compliance a condition of award.

Phase 1 has begun

4: Phase 1 is the initial stage where contractors will be required to conduct Level 1 and Level 2 self-assessments to demonstrate their compliance with cybersecurity requirements before contract award.

5: A C3PAO (Certified Third-Party Assessor Organization) is an independent company accredited by the [Cyber AB \(the CMMC Accreditation Body\)](#) to perform formal CMMC assessments.

6: DIBCAC (Defense Industrial Base Cybersecurity Assessment Center) is a unit within the Defense Contract Management Agency. It leads the Department of Defense's contractor cybersecurity risk-mitigation efforts by assessing contractors' compliance with cybersecurity requirements like [DFARS 252.204-7012](#) and [NIST SP 800-171](#).

7: Per the CMMC Final Rule, “CMMC requirements will be implemented using a 4-phase implementation plan over a three-year period”; however, the DoD extended Phase 1 from six months to a full year, pushing full implementation into 2028.

The most prepared suppliers are not waiting for CMMC enforcement. **They are de-risking their contracts now.**



They're doing this...

Submitting SPRS scores tied to defensible documentation

Identifying where CUI lives & flows in their environment

Validating controls using internal dry-runs

Getting leadership buy-in

Not this...

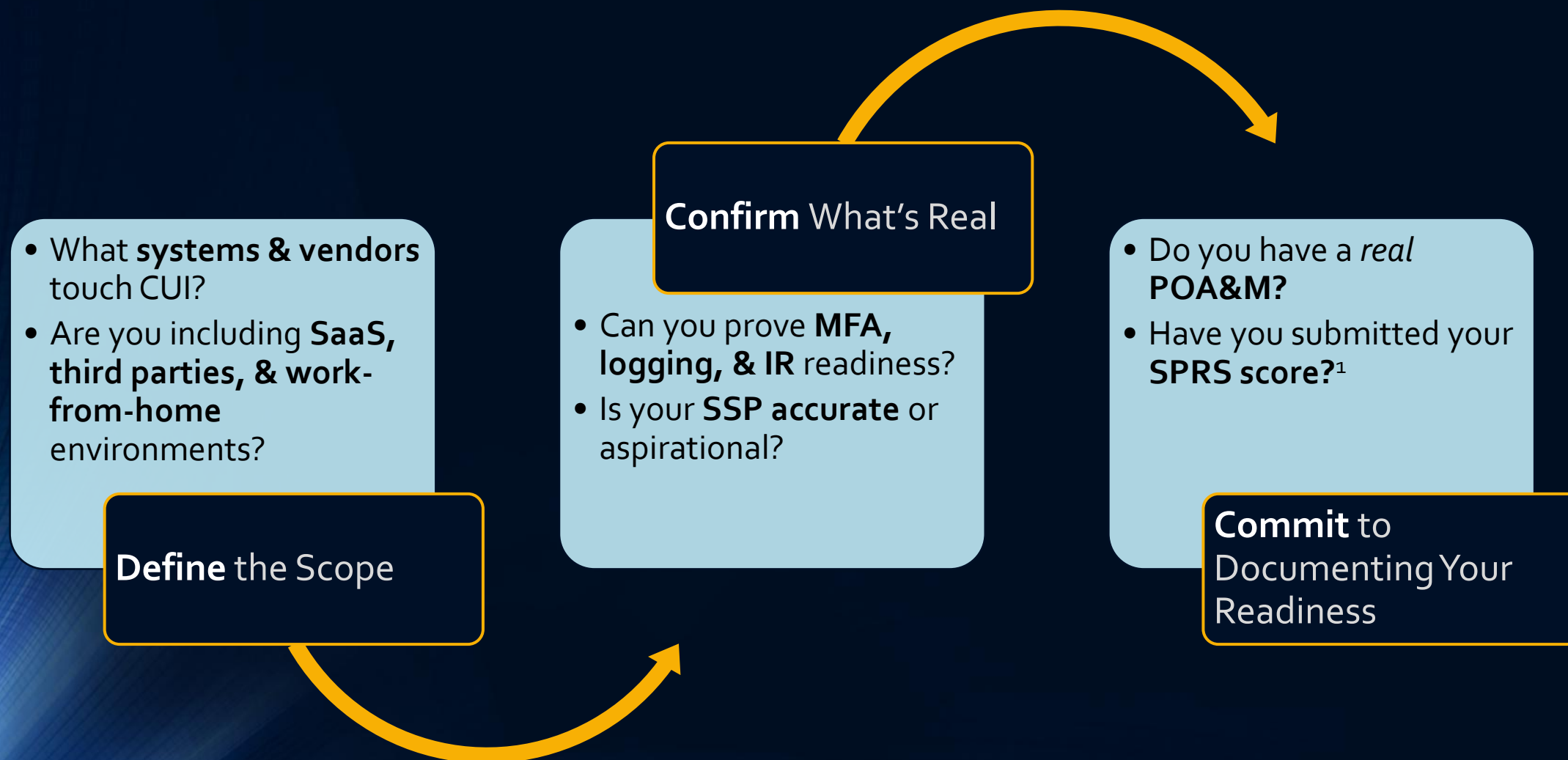
x Listing controls without showing how they're implemented

x Waiting for the RFP to spell out requirements

x Hoping a C3PAO will “just pass” them

x Treating CMMC as “the CISO’s job”

Three Moves That Keep You in the Game



1: SPRS is the Supplier Performance Risk System. It's the official DoD database where contractors must report their self-assessed NIST 800-171 compliance score. If your organization handles Controlled Unclassified Information (CUI), you're already required under [DFARS 252.204-7019](#) to perform a self-assessment using NIST SP 800-171, generate a score (based on the number of implemented controls), & upload that score to SPRS.

Define the Scope | If your scope is wrong, your controls & documentation will be too.

What systems & vendors touch CUI?

- Most organizations underestimate their exposure, especially with shared drives, old file shares, or legacy platforms still in use.
- When old drives or platforms still hold CUI, they are part of your attack surface.

Are you including SaaS, third parties, & work-from-home environments?

- If your SSP only describes your internal systems & ignores where the data actually travels, it's not CMMC-ready.
- Prime contractors are asking how you're securing remote access, personal devices, & SaaS apps because they are now a common part of the ecosystem.

Confirm what's real | If you can't prove it, it doesn't count.

Can you prove MFA, logging, & IR readiness?

- Saying “we have MFA” isn’t the same as proving enforcement across all accounts, including service accounts & vendors.
- Logging without review or retention means you’re not ready to respond.

Is your SSP accurate or aspirational?

- If your System Security Plan describes controls that aren’t fully implemented, & you don’t adjust your SPRS score accordingly, your score won’t hold up under scrutiny.
- Pre-assessments & prime reviews often fall apart when documentation tells one story & the environment reflects another.

Commit to Documenting Your Readiness | Documentation is a dealbreaker.

Do you have a *real* POA&M?

- A credible Plan of Action and Milestones includes timelines, ownership, & accountability.
- Primes & CMMC assessors want to see how you're closing the gaps you've already identified.

Have you submitted your SPRS score?

- Required today under DFARS 252.204-7019/7020
- If you haven't submitted your score, you may already be disqualified.

Prime contractors are asking for SPRS scores, SSPs, & proof of security controls now.

Subcontractors lacking documentation are being bypassed.

“,”

You don't need to be perfect, but **you do need to be provable.**

-VP of Contract Management, Federal Systems Integrator

We don't wait for contract language anymore. **We look at readiness up front.**

-Subcontracts Manager, Aerospace Prime

SPRS and a credible SSP are table stakes now. If you don't have both, you're not competitive.

-Cyber Risk Lead, Defense OEM

We turn **cybersecurity requirements** into **contract-readiness** to give you a **competitive edge**

Let's make your readiness real & provable. We can help you...

- ✓ Run self-assessments tied to verifiable controls
- ✓ Build SSPs & POA&Ms that stand up to scrutiny
- ✓ Close gaps with right-sized controls & documentation
- ✓ Align leadership, IT, Security & vendors around what matters most



ResilientTech Advisors

inquiries@resilienttechadvisors.com