PETRONELLA TECHNOLOGY GROUP

2026 EDITION · 24 PAGES

# CMMC 2.0 Readiness Guide

The 90-day roadmap to Level 1 or Level 2 certification, written by a CMMC Registered Practitioner.

Written by Craig Petronella · CMMC-RP · DFE #604180
A Registered Practitioner Organization accredited by the Cyber AB
petronellatech.com · (919) 348-4912

# Table of Contents

A practitioner-level walk-through of CMMC 2.0 — the rule, the mapping, the work, and the assessment.



## How to Use This Guide

If you have a current or upcoming DoD contract and you have seen CMMC language in a solicitation, this guide is for you. It is written for the person who will actually do the work — the IT lead, compliance manager, or owner-operator — not the procurement attorney.

Each chapter is self-contained. If you already know you are Level 1, skip Chapter 1 and go straight to Chapter 3. If you are building an SSP from scratch, read Chapters 2 and 4 together.

Primary source documents cited throughout: *32 CFR Part 170 (final rule, effective December 16, 2024), 48 CFR Part 204 (phased contract-clause rollout), DFARS 252.204-7012, NIST SP 800-171 Rev 3, NIST SP 800-172, and the Cyber AB Assessment Process Standard.*

# Chapter 1 · CMMC 2.0 Level 1 vs Level 2

## The three levels, in plain English

CMMC 2.0 collapsed the original five-level model into three. The vast majority of contractors will land at Level 1 or Level 2. Level 3 applies to a small subset handling the most sensitive CUI and is outside the scope of this guide.

| Level | Data Handled | Assessment | Control Set |
|---|---|---|---|
| **Level 1** | FCI (Federal Contract Information) | Annual self-assessment + annual affirmation | 15 basic safeguarding practices from FAR 52.204-21 |
| **Level 2** | CUI (Controlled Unclassified Information) | Triennial C3PAO assessment (or self-assessment for a narrow subset) + annual affirmation | 110 NIST SP 800-171 practices |
| **Level 3** | CUI + advanced persistent threat concerns | Triennial government-led (DIBCAC) assessment | 110 + selected NIST SP 800-172 enhancements |

## FCI vs CUI: the distinction that decides your level

**Federal Contract Information (FCI)** is information provided by or generated for the government under a contract that is not intended for public release. Think: SOWs, deliverables, non-public pricing.

**Controlled Unclassified Information (CUI)** is a broader, defined category spanning export-controlled technical data, OPSEC, critical infrastructure, defense information, and more. The authoritative list is the CUI Registry at archives.gov.

If your contract requires handling of CUI, you are a Level 2 target — regardless of company size.

> **COMMON SCOPING MISTAKE**

> Many small subcontractors assume they are Level 1 because they are small. The level is determined by the data in the contract, not by the size of your company. A two-person firm handling CUI is a Level 2 assessment. Read the contract clauses first.

## Why timing matters: the 48 CFR phased rollout

The 32 CFR Part 170 final rule (the "CMMC program rule") took effect on December 16, 2024. It establishes the program but does *not*, by itself, put CMMC clauses into contracts.

The companion 48 CFR rule — which amends the DFARS to actually insert CMMC requirements into solicitations — is being rolled out in four phases over three years:

- **Phase 1:** Self-assessment requirements appear in applicable solicitations.
- **Phase 2:** C3PAO (third-party) assessments required for Level 2.
- **Phase 3:** Level 3 assessments added.
- **Phase 4:** Full implementation — all applicable contracts carry CMMC requirements.

The practical implication: if you are in the defense industrial base, you should already be building toward your required level. Waiting for your contracting officer to tell you "you need CMMC now" is waiting too long — a Level 2 certification can take six to twelve months of preparation.

## Decision tree: what level am I?

1. Do you have a current or prospective DoD contract? — If no, CMMC likely does not apply.
2. Does the contract or solicitation include DFARS 252.204-7012, -7019, -7020, or -7021? — If yes, CMMC will apply.
3. Do you store, process, or transmit CUI (as defined by the CUI Registry)? — If yes → Level 2. If no, only FCI → Level 1.
4. Does the contract explicitly cite Level 3 or reference NIST SP 800-172? — If yes → Level 3 (beyond this guide).

> **ACTION THIS WEEK**
>
> Pull every active DoD contract and every open solicitation. Search for DFARS 252.204-7012 and CMMC. Write down your answer to the decision tree above. This single document becomes the front page of your SSP.

# Scoping: the single most common place CMMC projects fail

Scope is the set of people, processes, and technology that store, process, or transmit CUI. Every asset in scope is in your assessment. Every asset out of scope must be demonstrably isolated.

The final rule recognizes five categories of assets for Level 2 scoping:

- **CUI Assets** — process, store, or transmit CUI. Fully assessed.
- **Security Protection Assets (SPA)** — provide security functions (MFA, SIEM, firewall). Fully assessed.
- **Contractor Risk Managed Assets (CRMA)** — capable of handling CUI but controlled by policy to not. Documented, limited assessment.
- **Specialized Assets** — IoT, OT, test equipment, restricted platforms. Documented in SSP, not fully assessed.
- **Out-of-Scope Assets** — cannot process/store/transmit CUI. Must show segmentation.

> **WATCH OUT**
>
> If you cannot clearly articulate how an asset is segmented from CUI, an assessor will treat it as in scope. Network VLANs alone are rarely sufficient evidence — assessors look for firewall rules, directory boundaries, and documented policy.

## Enclave vs enterprise-wide: the strategic decision

You have two broad strategies:

- **Enclave:** Build a tightly-scoped environment that handles all CUI — often GCC High, a dedicated VDI, or a physically isolated network. Smaller assessment, faster to certify, but friction for users.
- **Enterprise-wide:** Treat the entire organization as in scope. Larger assessment, longer timeline, but no workflow friction and easier future-state posture.

Most small and mid-sized defense contractors choose the enclave strategy. The GCC High + dedicated device model has become the default pattern for organizations under 200 employees.

# Chapter 2 · NIST 800-171 Control Mapping

## The 14 control families

At Level 2, your assessment evaluates 110 practices organized into 14 control families. Each practice has one or more *assessment objectives*, and the assessor scores each objective as MET, NOT MET, or NOT APPLICABLE.

| Family | Abbr. | # of Practices | Emphasis |
|---|---|---|---|
| Access Control | AC | 22 | Identity boundaries, least privilege |
| Awareness & Training | AT | 3 | Role-based security training |
| Audit & Accountability | AU | 9 | Logging, log review, retention |
| Configuration Management | CM | 9 | Baselines, change control, inventory |
| Identification & Authentication | IA | 11 | MFA, password policy, device ID |
| Incident Response | IR | 3 | Plan, test, report |
| Maintenance | MA | 6 | Sanitization, remote maintenance control |
| Media Protection | MP | 9 | Marking, transport, destruction |
| Personnel Security | PS | 2 | Screening, termination |
| Physical Protection | PE | 6 | Facility access, escorting |
| Risk Assessment | RA | 3 | Periodic risk + vulnerability scans |
| Security Assessment | CA | 4 | Control testing, POA&M |
| System & Communications Protection | SC | 16 | Network boundary, encryption, FIPS |
| System & Information Integrity | SI | 7 | Flaw remediation, anti-malware, monitoring |

**SCORING NOTE**

DoD uses the NIST 800-171 DoD Assessment Methodology scoring: start at 110, subtract point values (1, 3, or 5) for unmet practices. A perfect score is 110. You must score at or above 88 to certify at Level 2, with the remaining ≤22 points of gaps captured in a POA&M that must be closed within 180 days.

# What "adequate security" under DFARS 252.204-7012 means today

DFARS 252.204-7012 predates CMMC and is the clause that originally required defense contractors handling Covered Defense Information (a superset of CUI) to implement NIST SP 800-171.

Practically, this means: if you hold DoD contracts today, you are already contractually obligated to have the 110 controls of NIST 800-171 implemented. CMMC 2.0 Level 2 is the verification mechanism for that existing obligation — not a new requirement.

The 7012 clause also requires:

- Reporting cyber incidents to DoD within 72 hours of discovery (to dibnet.dod.mil).
- Submission of malicious software to DoD Cyber Crime Center (DC3) when isolated.
- Preservation of images of affected systems for at least 90 days.
- Flow-down of the clause to subcontractors who also handle CDI.

# High-leverage controls: where most gaps live

In our experience as a Registered Practitioner Organization preparing clients for Level 2, four families account for the majority of "Not Met" findings:

1. **Audit & Accountability (AU):** Organizations collect logs but cannot show that they are reviewed. Practice 3.3.5 (correlation) and 3.3.6 (reporting) are frequently missed without a SIEM.
2. **System & Communications Protection (SC):** FIPS 140-validated cryptography is a common gap. "We use TLS" is not sufficient — you must be able to point to the FIPS certificate for the module.
3. **Configuration Management (CM):** Authoritative device inventory, a baseline configuration standard per OS, and change-approval evidence.
4. **Identification & Authentication (IA):** Phishing-resistant MFA at every boundary, including VPN, remote maintenance, and cloud admin consoles.

# Assessment objectives: the real unit of scoring

Each of the 110 practices decomposes into one or more *assessment objectives* drawn from NIST SP 800-171A (the assessment procedures document). Objectives are stated as propositions the assessor verifies.

Example — Practice 3.1.1 (Access Control) has six objectives:

1. [a] Authorized users are identified.
2. [b] Processes acting on behalf of authorized users are identified.
3. [c] Devices (and other systems) authorized to connect are identified.
4. [d] System access is limited to authorized users.
5. [e] System access is limited to processes acting on behalf of authorized users.
6. [f] System access is limited to authorized devices (including other systems).

To score MET on 3.1.1, all six objectives must be independently met. Missing a single objective fails the practice.

> **EVIDENCE RULE OF THREE**
>
> For each practice, prepare three forms of evidence: (1) the written policy, (2) a procedure or runbook showing how the policy is executed, and (3) an artifact proving the procedure ran (log export, ticket, signed acknowledgment). Assessors look for all three.

# Shared responsibility in cloud environments

If you host CUI in a cloud service (M365 GCC High, Azure Government, AWS GovCloud), the cloud provider inherits some controls. You must:

- Obtain the Customer Responsibility Matrix (CRM) from the provider.
- Document, for each practice, whether it is "Inherited", "Shared", or "Customer".
- Verify the provider holds a FedRAMP Moderate (or Moderate-equivalent) authorization for CUI under DFARS 7012(b)(2)(ii)(D).

# Chapter 3 · The 90-Day Readiness Roadmap

This is the sequence our Registered Practitioner team uses with clients targeting Level 2. Adjust calendar weeks to your own — the ordering matters more than the exact dates.

## Weeks 1 – 2: Scope & foundations

WEEK 1

### Confirm level, build the asset inventory, flag CUI

- Complete the Chapter 1 decision tree; write the one-page scoping memo.
- Inventory every endpoint, server, network device, SaaS tenant, and specialized asset. Tag each with its asset category (CUI / SPA / CRMA / Specialized / Out-of-Scope).
- Identify every place CUI can land: email, file shares, ERP, CAD, email, endpoints of remote users.

WEEK 2

### Commission the enclave (if enclave strategy)

- Stand up GCC High tenant or Azure Government workload with dedicated identities.
- Configure data-loss prevention (DLP) rules to quarantine CUI leaving the enclave.
- Deploy enclave-only endpoints (Autopilot + conditional access) to the handful of users who will touch CUI.

# Weeks 3 – 4: Gap assessment

WEEK 3

### Score yourself against all 110 practices

- Use the NIST 800-171 DoD Assessment Methodology to produce a baseline score.
- For each practice, record: objective status, evidence available today, owner, estimated effort.
- Output: a gap register in a spreadsheet, one row per assessment objective (~320 rows).

WEEK 4

### Prioritize remediation

- Group gaps by family; tackle IA and AC first (highest point values, most dependencies).
- Identify which gaps can be policy-only, which require tooling, and which require process change.
- Draft the SPRS (Supplier Performance Risk System) score you will submit post-remediation.

## Weeks 5 – 6: Policy & procedure authoring

WEEK 5

### Write the 14 family policies

- One policy per family, signed by an executive. Policies answer "what we require" — not how.
- Treat the policy as the backstop for every control. No control should exist without a policy reference.

WEEK 6

### Write the procedures (the "how")

- Procedures are step-by-step runbooks: onboarding, offboarding, patch approval, incident response, media disposal.
- Every procedure names the role responsible, the cadence, and the evidence produced.

## Weeks 7 – 8: Identity, encryption, boundary

WEEK 7

### MFA, password policy, conditional access

- Enable phishing-resistant MFA (FIDO2, CBA, or Windows Hello for Business) for every CUI and SPA user.
- Block legacy authentication protocols. Remove service accounts from interactive logon.
- Document the IA decisions in the SSP sections IA-2 through IA-11.

WEEK 8

### FIPS-validated cryptography & boundary protections

- Confirm every cryptographic module protecting CUI holds a FIPS 140-2 or 140-3 validation. Record certificate numbers.
- Configure firewall rules by default-deny, log denies, document the boundary protection architecture in SSP SC sections.
- Enable full-disk encryption on every endpoint in scope.

## Weeks 9 – 10: Logging, monitoring, incident response

WEEK 9

### SIEM / log aggregation

- Forward logs from every in-scope system to a central SIEM. Retain ≥90 days online, ≥1 year archive.
- Define alert rules for: privileged-account use, logon failures, new admin, DLP triggers, EDR high-severity.
- Document who reviews alerts, how often, and the escalation path. This closes AU-3.3.5/6 gaps.

WEEK 10

### Incident response plan + tabletop

- Write an IR plan that names detection, containment, eradication, recovery, and post-incident roles.
- Include the DFARS 72-hour reporting flow to dibnet.dod.mil.
- Run one tabletop exercise. Capture the minutes — the minutes are your IR-3.6.3 evidence.

## Weeks 11 – 12: Training, evidence, pre-assessment

WEEK 11

### Role-based security training + completion records

- Deliver baseline security awareness to every user in scope.
- Deliver role-based training to privileged users (admins, incident responders, insider-threat custodians).
- Archive completion records with names and dates. This closes the AT family.

WEEK 12

### Internal readiness assessment (dry run)

- Run a full mock assessment against all 110 practices and ~320 objectives.
- For every unmet objective, either remediate or add to the POA&M (see Chapter 5 for rules on what can and cannot go on the POA&M).
- Finalize the SSP and POA&M. You are now ready to engage a C3PAO.

**REALISTIC EXPECTATIONS**

Ninety days is an aggressive pace for an organization starting from zero. Most of our clients extend to 120 – 180 days. The sequence above is what matters — compress or stretch the calendar around it.

# Cost anchors: what to budget for

We avoid publishing fabricated averages — every environment is different. Use these categories to build your own budget:

- **Enclave tenancy** — GCC High per-user licensing + Entra ID P2. Recurring.
- **Endpoint hardening** — EDR with behavioral detection, disk encryption management. Recurring.
- **Identity** — FIDO2 keys (or equivalent) for every user in scope. One-time + replacements.
- **SIEM / log retention** — either subscription SIEM or self-hosted with cold storage. Recurring.
- **Advisory / RPO support** — gap assessment, SSP authoring, mock assessment. Usually fixed-fee projects.
- **C3PAO assessment fee** — triennial. Varies by scope and assessor.
- **Remediation surprises** — budget a contingency for the discoveries you will make in Week 3.

Ask your C3PAO for a scoping call *before* you engage them so the assessment fee is predictable. Assessors want to see your SSP and asset inventory first.

## Funding signals to watch

- APEX Accelerators (formerly PTAC) sometimes offer CMMC readiness grants in specific states.
- DoD Mentor-Protégé Program agreements can fund CMMC investment.
- The NIST MEP (Manufacturing Extension Partnership) has a network focused on DIB cybersecurity assistance.

Verify current funding availability directly with the program — these programs change year to year.

# Chapter 4 · SSP Template Walkthrough

The System Security Plan (SSP) is the single most-examined artifact in a Level 2 assessment. A strong SSP walks the assessor through your boundary, your controls, and your decisions — so the assessor spends their time verifying, not decoding.

## Recommended SSP outline

1. **Section 1: System identification** — system name, owner, authorizing official, assessment scope.
2. **Section 2: System description** — purpose, data types handled, user populations.
3. **Section 3: System boundary & architecture** — a single authoritative network diagram showing CUI flow, enclaves, and boundary devices.
4. **Section 4: Asset inventory** — every asset by category (CUI / SPA / CRMA / Specialized / Out-of-Scope).
5. **Section 5: Roles & responsibilities** — named individuals for security, privacy, IR, configuration management.
6. **Section 6: Control implementation (14 families)** — described below.
7. **Section 7: Continuous monitoring strategy** — how and how often each control is verified in production.
8. **Section 8: POA&M reference** — pointer to the current POA&M (Chapter 5).
9. **Section 9: Appendix A — policies**. Attach or reference.
10. **Section 10: Appendix B — procedures**. Attach or reference.

> **WRITING TIP**
>
> Section 6 should be written *per assessment objective*, not per practice. Each objective gets its own paragraph and its own evidence reference. This is the single change that cuts assessment time most.

# Section 6 control-family template (fill one per family)

FAMILY: ACCESS CONTROL (AC) — 22 PRACTICES

### Policy reference

Cite the access-control policy document, version, and date of last executive approval.

### Scope & inheritance

Which assets are subject to this family. Which objectives are inherited from cloud providers (with CRM reference).

### Practice-by-practice implementation

For each of the 22 practices (3.1.1 – 3.1.22), one paragraph per assessment objective describing how the objective is met and what evidence proves it.

### Evidence index

A table linking each objective to the specific log query, configuration export, or signed document that proves it.

FAMILY: IDENTIFICATION & AUTHENTICATION (IA) — 11 PRACTICES

### Policy reference

Cite identity, MFA, and password policies.

### MFA posture

Describe the authenticator class (FIDO2, CBA, Windows Hello for Business, TOTP) and which user populations use which. Phishing-resistant by default; document any exceptions.

### Privileged accounts

Describe separation of privileged from standard accounts, just-in-time elevation, and break-glass procedure.

### Evidence index

Conditional-access policies, sign-in logs proving MFA, password-policy export.

FAMILY: AUDIT & ACCOUNTABILITY (AU) — 9 PRACTICES

### Logging architecture

Which systems forward to SIEM, retention targets, storage integrity controls.

### Review cadence

Who reviews alerts, on what schedule, using what runbook. The SIEM's alert history is your evidence for 3.3.5 (correlation) and 3.3.6 (reporting).

### Evidence index

Retention policy screenshots, alert rules export, sample ticket showing review and escalation.

FAMILY: SYSTEM & COMMUNICATIONS PROTECTION (SC) — 16 PRACTICES

### Boundary protection

Firewall model, default-deny posture, rule-review cadence, documented exceptions with business justification.

### Cryptography

For each cryptographic module protecting CUI, record the FIPS 140-2 or 140-3 certificate number and the module's status (Active / Historical). CUI-in-transit and CUI-at-rest are evaluated separately.

### Segmentation

How CUI traffic is isolated from other traffic. Evidence: network diagram + ACL export.

FAMILY: SYSTEM & INFORMATION INTEGRITY (SI) — 7 PRACTICES

### Flaw remediation

Patch tiers, SLAs by severity, evidence of patch deployment (compliance report from your patch tool).

### Malicious code protection

EDR tool, behavior-based detection, update cadence, quarantine flow.

### Monitoring

Alert sources, SIEM integration, named roles.

## The other 9 families: apply the same pattern

AT, CM, IR, MA, MP, PS, PE, RA, CA all get the same structure: policy → implementation description per objective → evidence index. The goal is that an assessor can read the SSP, open your evidence folder, and verify in one pass.

> **COMMON SSP FAILURE MODE**
>
> The SSP says "we comply with 3.1.5." That is not a description — that is a restatement. Assessors need the *how*: what tool, what setting, what role, what evidence. Vague SSPs force rework and lengthen assessments.

# Chapter 5 · POA&M Best Practices

A Plan of Action & Milestones (POA&M) documents unmet controls and the plan to close them. Under 32 CFR Part 170, limited POA&Ms are permitted at Level 2 but with strict conditions.

## What CAN appear on a Level 2 POA&M

- Any practice scored as NOT MET **except** those explicitly disallowed.
- Your total POA&M deductions cannot exceed the point total equivalent to your final score of ≥88.
- All POA&M items must be closed and re-evaluated within 180 days of the assessment.

## What CANNOT appear on a Level 2 POA&M

The final rule identifies specific practices that cannot be on a POA&M at Level 2 — they must be MET at assessment or the assessment fails. The current list includes:

- All 5-point (highest-weight) practices.
- Specifically-named 3-point practices covering MFA, authenticator management, and incident reporting.

Check the current Cyber AB Assessment Process Standard for the authoritative list — the exclusion list can evolve.

> **DO NOT TRY TO POA&M THE HARD STUFF**
>
> If MFA or incident reporting is not fully met at assessment time, your assessment fails. Plan your 90 days so that these practices are rock-solid before the C3PAO arrives.

## POA&M item structure

Each item on your POA&M should contain:

1. Practice and objective identifier.
2. Description of the gap (what objective is unmet, why).
3. Planned corrective action (concrete, testable).
4. Named owner (person, not team).

5. Resources required (licenses, budget, labor).
6. Milestones (intermediate dates, not just a final due date).
7. Status (Open / In Progress / Closed-Pending-Verification / Closed).
8. Expected closure date (≤ 180 days from assessment date).

## Closing POA&M items: what assessors look for

Closing a POA&M item is not just marking it "done." The assessor will require:

- An artifact proving the corrective action was implemented (screenshot, report, signed approval).
- An artifact proving the control now operates in production (a log entry, an alert, a completion record).
- A policy or procedure update if the control's sustainment changed.
- Re-evaluation of the practice by the same assessor team (usually a desk review, not a full re-visit).

## POA&M governance

Treat the POA&M as a living document:

- Review it monthly at a leadership level — not just by IT.
- Raise slipping milestones to the authorizing official (AO).
- Audit closed items quarterly — make sure closed controls have not silently regressed.

## Linking SSP and POA&M

Your SSP Section 8 should be a table of open POA&M items with their due dates. Your POA&M should reference the SSP section and assessment objective number. Assessors frequently cross-check the two documents; misalignment is a finding.

> **PRACTICAL TEMPLATE**
>
> Keep the POA&M in a single spreadsheet with one row per item and these columns: ID, Practice, Objective, Gap, Corrective Action, Owner, Milestones, Status, Due Date, Closure Evidence. Use cell comments to link to the evidence folder.

# Chapter 6 · C3PAO Assessment Prep

## Choosing a C3PAO

A C3PAO (CMMC Third-Party Assessor Organization) is the only entity that can certify you at Level 2. Authorization is managed by the Cyber AB.

- Pull the current list from the Cyber AB marketplace.
- Verify "Authorized" status, not "Candidate." Only Authorized C3PAOs can perform assessments under 32 CFR Part 170.
- Ask for references in your sector (aerospace, shipbuilding, electronics manufacturing, etc.).
- Confirm the lead assessor is a Certified CMMC Professional (CCP) and that the team includes a Certified CMMC Assessor (CCA).
- Request a scoping call so the fee is based on actual asset count, not an abstract estimate.

> **INDEPENDENCE RULE**
>
> A C3PAO cannot assess an organization it has also provided consulting to. If your advisory partner is a Registered Practitioner Organization (RPO) such as Petronella, they are explicitly *not* the assessor — they prepare you, and an independent C3PAO certifies you.

## What to stage before kick-off

1. Final SSP (all 14 families, per-objective descriptions).
2. Asset inventory spreadsheet with categorizations.
3. Evidence folder, organized by practice and objective.
4. Policy set (14 signed policies).
5. Procedure / runbook library.
6. POA&M (spreadsheet).
7. Network architecture diagram (single authoritative source).
8. Personnel roster showing role assignments for security, privacy, IR.
9. Training completion records.
10. Vendor artifacts: FedRAMP status letters, CRMs, FIPS certificates.

## Assessment phases

1. **Plan & prepare.** Scoping call, contract, evidence upload.
2. **Conduct.** Interviews, evidence examination, technical testing. Typically on-site or hybrid, one to two weeks depending on scope.
3. **Report.** Draft assessment report with scoring.
4. **Remediate (if needed).** Up to 180 days to close POA&M items.
5. **Certify.** Final report uploaded to SPRS; status visible to contracting officers.

## How scoring works in the room

For each practice, the assessor interviews the owner, examines evidence, and tests the control technically where possible. Outcomes per objective:

- **MET** — all objectives verified. Practice counts for full points.
- **NOT MET** — at least one objective unverified. Practice deducts its point value from 110.
- **NOT APPLICABLE** — assessor and contractor agree the practice does not apply (e.g., no wireless in the environment for 3.1.16). N/A practices do not deduct points but the rationale is documented.

## After certification: staying certified

- **Annual affirmation** — a senior official affirms continued compliance each year.
- **Continuous monitoring** — the practices must continue to operate in production, not just during the assessment week.
- **Change management** — significant architectural changes may require re-assessment before the 3-year cycle.
- **Triennial re-assessment** — another C3PAO assessment at the 3-year mark.

> **DO NOT DECAY**
>
> The most common reason organizations fail re-assessment is quiet decay: logging silently breaks, MFA exceptions creep in, an inventory goes stale. Build continuous monitoring into your calendar.

# Chapter 7 · Why a Registered Practitioner Org Matters

The Cyber AB recognizes three kinds of ecosystem partners:

- **Registered Practitioners (RP)** and **Registered Practitioner Organizations (RPO)** — can consult, advise, and prepare you for assessment. Cannot certify.
- **Certified CMMC Professionals (CCP)** — advanced individual credential, often on C3PAO teams.
- **Certified CMMC Assessors (CCA)** and **C3PAOs** — can certify.

## What an RPO brings that a generic MSP does not

- **Code of Professional Conduct** — RPOs operate under the Cyber AB CoPC, with disclosure and independence obligations.
- **Training continuity** — RPs take formal training on the CMMC Model, NIST 800-171, and the Assessment Process Standard.
- **Evidence discipline** — RPs work backward from what assessors will want to see, not forward from what the firewall can do.
- **Relationships with C3PAOs** — RPOs know which C3PAOs assess which sectors, which helps scoping calls be predictable.

## Independence: the bright line

Under the final rule, the entity that advises you is not the entity that certifies you. A good RPO will make the hand-off clean: they prepare your SSP, your evidence, your mock assessment — then step back while an independent C3PAO does the real assessment.

> **PETRONELLA'S POSTURE**
>
> Petronella Technology Group is a Registered Practitioner Organization accredited by the Cyber AB. The entire Petronella cybersecurity team holds the CMMC-RP credential. Our role is preparation, documentation, remediation, and mock assessment — with a clean hand-off to an independent C3PAO for certification.

# Chapter 8 · About Petronella Technology Group

Petronella Technology Group is a Raleigh, North Carolina cybersecurity and compliance firm founded in 2002. We operate as a Registered Practitioner Organization accredited by the Cyber AB and hold a BBB A+ rating since 2003.

## What we do

- **CMMC readiness** — gap assessment, SSP authoring, evidence packaging, mock assessment.
- **NIST 800-171 & 800-172 implementation** — policy, procedure, and control rollout.
- **Managed security** — 24/7 monitoring, incident response, EDR, email security.
- **Digital forensics** — breach response, evidence preservation, DoD DFARS 7012 72-hour reporting support.
- **Compliance-aligned managed IT** — HIPAA, FTC Safeguards, SOC 2 Type II, PCI DSS.

## Who we are

**Craig Petronella**, Founder & CEO.
Credentials: CMMC-RP, CCNA, CWNE, DFE #604180. Author of several books on cybersecurity and compliance for small business.

The cybersecurity team holds the CMMC Registered Practitioner credential. Engagements are led by an RP and supported by engineers with specific expertise in cloud compliance (GCC High, Azure Government), identity (Entra ID, conditional access), and SIEM.

## How to reach us

**Phone:** (919) 348-4912
**Web:** petronellatech.com
**Office:** 5540 Centerview Dr, Raleigh, NC 27606
**Email:** sales@petronellatech.com

### Further reading on our CMMC capability

- CMMC compliance services

- CMMC assessment preparation
- ComplianceArmor documentation engine

# Chapter 9 · Sources & Further Reading

Every factual claim in this guide can be traced back to one of the following primary sources. For any point where regulation and this guide disagree, *the regulation is authoritative*.

## Primary regulatory sources

- **32 CFR Part 170** — CMMC Program final rule (effective December 16, 2024). ecfr.gov
- **48 CFR / DFARS 252.204-7012, -7019, -7020, -7021** — contract-clause requirements for safeguarding, assessment, and CMMC certification. acquisition.gov
- **NIST SP 800-171 Rev 3** — Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. csrc.nist.gov
- **NIST SP 800-171A** — Assessing Security Requirements for CUI (the objectives document).
- **NIST SP 800-172** — Enhanced Security Requirements (Level 3).
- **CUI Registry** — authoritative CUI categories. archives.gov/cui

## Program governance

- **Cyber AB** (accreditation body for CMMC). cyber-ab.org
- **Cyber AB Assessment Process Standard** — the operative procedure document for assessments.
- **DoD Cyber Crime Center (DC3)** — malicious software submission. dc3.mil
- **DIBNet** — 72-hour incident reporting portal. dibnet.dod.mil
- **SPRS** — Supplier Performance Risk System (where scores live). sprs.csd.disa.mil

## Ecosystem resources

- NIST MEP (Manufacturing Extension Partnership) DIB cybersecurity resources.
- APEX Accelerators (formerly PTAC) — state-level assistance programs.
- DoD Mentor-Protégé Program.

> **REGULATION MOVES**

> CMMC is a living program. The 48 CFR phase dates, the POA&M exclusion list, and assessor-marketplace composition evolve. Revisit primary sources before committing to specific dates.

# Ready to move from reading to doing?

If this guide helped, the next step is a working session with a Registered Practitioner. We spend 60 minutes on your scope, your gaps, and a concrete 90-day plan — free, no obligation.

**(919) 348-4912**

petronellatech.com/contact-us

**Petronella Technology Group**
5540 Centerview Dr, Raleigh, NC 27606 · Registered Practitioner Organization · BBB A+
Since 2003