FOR DEFENSE INDUSTRIAL BASE SUB-PRIMES

CMMC Scoping Worksheet

A 12-Step Guide to Determine Your CMMC Scope

Map your in-scope assets, users, and data flows in 45 minutes, then schedule a free CMMC scoping consultation with a CMMC-RP.

Levels 1, 2 and 3

Scope every CMMC level, including Level 3 (Expert).

Built for sub-primes

Flow-down obligations, enclaves, FCI versus CUI.

No pricing pressure

Custom-quote model. Scope drives the engagement.

Petronella Technology Group, Inc.

CMMC-AB Registered Provider Organization #1449
5540 Centerview Dr., Suite 200, Raleigh, NC 27606

(919) 348-4912 | petronellatech.com

How to Use This Worksheet

This worksheet is a structured 45-minute scoping exercise for Defense Industrial Base (DIB) sub-prime contractors preparing for, or actively pursuing, a contract that requires Cybersecurity Maturity Model Certification (CMMC) compliance.

It is not a self-assessment. It is a scoping intake that produces enough signal for Petronella Technology Group, Inc. to estimate a realistic engagement length when you schedule a free 30-minute scoping consultation.

Time budget

- ☐ 45 minutes, single sitting, one organization.
- ☐ If you cannot answer a question, leave it blank. Blank answers are diagnostic in their own right.

Have ready before you start

- ☐ Current organization chart (IT, security, and contracts roles especially).
- ☐ IT inventory: endpoints, servers, network devices, SaaS subscriptions.
- ☐ Current or anticipated DoD contracts with DFARS clauses highlighted:
  - DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
  - DFARS 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements
  - DFARS 252.204-7020 NIST SP 800-171 DoD Assessment Requirements
  - DFARS 252.204-7021 Cybersecurity Maturity Model Certification Requirements
- ☐ Points of contact for IT operations, information security, and contracts management.

What a completed worksheet gives you

1. A clear picture of your in-scope assets, users, and data flows.
2. A working hypothesis of which CMMC level applies to your organization.
3. A self-scored engagement bracket framed by typical project length, not dollars.

What happens next

1. Email your completed worksheet to your scoping coordinator (see the Next-Step Checklist).
2. Schedule a free 30-minute scoping consultation.
3. On the call, Petronella Technology Group, Inc. delivers an engagement-length estimate and a proposed scope of work. No pricing pressure on the call. We do not publish fixed CMMC pricing because the scope drives everything.

The 12 Scoping Questions

Answer each question for one organization. Check every box that applies and fill the open fields. Leave blanks where you are unsure - blanks are diagnostic too.

Q1 DoD Contracting Status

What is your current relationship to DoD contracting?

- ☐ **Prime contractor. You hold the direct DoD contract.**
- ☐ **Sub-prime, tier 1. You sub-contract directly to a prime.**
- ☐ **Sub-prime, tier 2 or deeper. You sub-contract to a sub-prime.**
- ☐ **Pursuing first DoD contract. No active award, but bidding.**
- ☐ **Sole-source-eligible. Special vehicle or pre-qualified pool.**
- ☐ **Set-aside designation. Check all that apply below.**
  - ☐ WOSB (Women-Owned Small Business)
  - ☐ SDVOSB (Service-Disabled Veteran-Owned Small Business)
  - ☐ 8(a) Business Development Program
  - ☐ HUBZone

> Why this matters: Your tier and set-aside status affect flow-down obligations and which DFARS clauses your prime is contractually required to push down to you. Sub-primes are increasingly required to inherit the prime's CMMC level rather than self-determining.

Q2 CMMC Level Required

What CMMC level does your current or anticipated contract require?

- ☐ **Level 1 Foundational. 17 practices, annual self-assessment.**
- ☐ **Level 2 Advanced. 110 practices aligned to NIST SP 800-171; triannual C3PAO assessment for most CUI contracts.**
- ☐ **Level 3 Expert. Level 2 plus a subset of NIST SP 800-172 controls; triannual government-led assessment.**
- ☐ **Not yet specified. I do not know.**

If you do not know, there are two paths to find out:

1. Re-read your contract for DFARS clauses 252.204-7012 and 252.204-7021. Clause 7021 references the applicable CMMC level when present.
2. Ask your Contracting Officer or Contracting Officer's Representative for the CMMC level requirement in writing.

> Why this matters: Many contracts that historically required only DFARS 7012 will be upgraded to require Level 2 certification as CMMC rolls out across DoD acquisitions.

Q3 Data Types Handled

What categories of federal data does your organization handle? Check all that apply.

- ☐ **FCI only (Federal Contract Information). Information provided by or generated for the government under a contract, not intended for public release. Likely Level 1.**
- ☐ **CUI (Controlled Unclassified Information). Sensitive but unclassified information requiring safeguarding under federal law, regulation, or government-wide policy. Level 2 minimum.**
- ☐ **CUI Specified. CUI categories with additional handling controls beyond CUI Basic (CDI, CTI, NNPI, Defense Critical Infrastructure Security Information). Level 2 with elevated controls.**
- ☐ **APT-targeted CUI. CUI that DoD has flagged as a likely target of Advanced Persistent Threats. Often drives Level 3.**
- ☐ None of the above, or unsure.

Authoritative reference: the National Archives CUI Registry catalogues every CUI category and subcategory at archives.gov/cui, with the DoD CUI program portal at dodcui.mil.

> Why this matters: Data type drives level. Sub-primes frequently mis-classify FCI as CUI (over-scoping, more cost) or CUI as FCI (under-scoping, contract risk). A scoping consultation can resolve disputed classifications.

Q4 Headcount Touching FCI or CUI

How many employees, contractors, and consultants can access, process, store, or transmit FCI or CUI?

- ☐ 1 to 10
- ☐ 11 to 50
- ☐ 51 to 200
- ☐ 200 or more

Of that headcount, how many are remote or hybrid workers using endpoints outside a corporate-managed network?

Remote or hybrid users: _____

> Why this matters: Headcount drives the scope of awareness training, access reviews, audit log volume, and identity infrastructure. A remote workforce expands the in-scope boundary and typically increases the controls burden.

Q5 IT Infrastructure Handling FCI or CUI

Where does FCI or CUI live, move, or get processed in your environment? Check all that apply.

- ☐ **On-premises servers. File shares, application servers, databases.**
- ☐ **Cloud infrastructure. Specify provider and tier below.**
  - ☐ AWS GovCloud (US)
  - ☐ Microsoft Azure Government
  - ☐ Microsoft 365 GCC High
  - ☐ Microsoft 365 GCC (not High)
  - ☐ Google Workspace (commercial)
  - ☐ Commercial cloud (non-government tenant)
- ☐ **Hybrid. Mix of on-prem and cloud.**
- ☐ **SaaS tools. List every SaaS product that touches FCI or CUI (CRM, document storage, file transfer, e-signature, ticketing, project management, code repository, video conferencing):**

Why this matters: Every system that stores, processes, or transmits CUI is in-scope for CMMC. SaaS tools are the most common scoping surprise. A single non-compliant SaaS in the CUI flow can put the entire assessment at risk. Commercial cloud (non-government tenant) is generally not acceptable for CUI under the DFARS 252.204-7012 cloud requirements.

Q6 Enclaves and Boundaries

How is your CUI environment segmented from the rest of your IT estate?

- ☐ **No segmentation. CUI lives alongside general business data.**
- ☐ **Logical network segmentation. VLANs, ACLs, or firewall rules separate CUI systems.**
- ☐ **Dedicated VLAN or subnet. For CUI workloads.**
- ☐ **Physical air-gap. Hardware-isolated CUI environment.**
- ☐ **Dedicated cloud tenant. Isolated from production business workloads.**
- ☐ **GCC High enclave. Conditional access policies restricting CUI to enclave users.**
- ☐ **Microsoft 365 enclave architecture. Restricted SharePoint sites, Teams, OneDrive, and Exchange isolated from commercial tenants.**

Why this matters: A well-designed enclave dramatically reduces the in-scope footprint. Scoping work often pays for itself by shrinking the assessment surface from the entire company to the enclave plus the users with enclave access.

Q7 Current Security Posture

What is your current cybersecurity program maturity?

- ☐ **No formal program. Ad-hoc security, no documented policies.**
- ☐ **Some controls in place, But no System Security Plan (SSP).**
- ☐ **SSP exists but is stale. Last updated more than 12 months ago.**
- ☐ **SSP current. Updated within 12 months, with a Plan of Action and Milestones (POA&M) tracking open gaps.**
- ☐ **SSP current plus independent assessment. A third party (RPO, C3PAO, or internal audit) has reviewed the SSP and evidence within 12 months.**
- ☐ **SPRS score posted. A NIST SP 800-171 self-assessment score is submitted in the Supplier Performance Risk System.**

Current SPRS score (range -203 to 110): _____

Why this matters: Posture drives the gap-assessment timeline. Organizations without an SSP need an SSP-first engagement. Organizations with a current SSP plus POA&M typically need a remediation engagement plus a mock assessment.

Q8 Identity and Access Management

How do users authenticate to systems that handle FCI or CUI?

- ☐ **Shared accounts. Multiple users share login credentials.**
- ☐ **Per-user accounts with passwords only. No multi-factor.**
- ☐ **MFA on critical systems only. Email, VPN, key applications only.**
- ☐ **MFA everywhere. On all systems that access FCI or CUI.**
- ☐ **Zero-trust identity architecture. Conditional access, device compliance enforcement, continuous verification.**

Privileged access: are administrative and privileged accounts separated from standard user accounts?

- ☐ Yes, fully separated with privileged access management (PAM).

- ☐ Partially separated, no PAM tooling.
- ☐ No separation. Admins use one account for everything.

> Why this matters: CMMC Level 2 requires MFA on all CUI access, separation of privileged accounts, and unique identification of every user. Shared accounts are an automatic finding.

Q9 Logging and Monitoring

How does your organization collect, retain, and review security logs?

- ☐ No centralized logging.
- ☐ **Endpoint logs only. Windows Event Logs or equivalent, not aggregated.**
- ☐ **Centralized SIEM. Log aggregation but no continuous monitoring.**
- ☐ **SIEM plus 24/7 monitoring. Internal SOC or managed detection and response (MDR) provider.**
- ☐ **SIEM plus monitoring plus IR retainer. With a qualified incident-response firm on standby.**

Log retention period (days). Level 2 commonly interpreted as 90 days minimum online:

Date of last security log review (or 'never'):

> Why this matters: The CMMC Audit and Accountability (AU) family contains controls that require significant logging infrastructure. Sub-primes routinely under-scope this. Logs without review do not satisfy AU controls.

Q10 Vulnerability and Patch Management

How do you identify and remediate vulnerabilities in systems that handle FCI or CUI?

- ☐ **Ad-hoc. No scheduled scanning or patching cadence.**
- ☐ **Quarterly vulnerability scans. With informal remediation.**
- ☐ **Monthly scans. With a documented patching cadence.**
- ☐ **Continuous scanning. With a defined patch SLA (for example, critical vulnerabilities patched within 72 hours).**
- ☐ **Continuous scanning plus configuration management. With deviations alerted and tracked.**

Patch SLA for critical vulnerabilities (days):

> Why this matters: CMMC Level 2 has explicit cadence requirements for vulnerability scanning and patching under the Risk Assessment (RA) and System and Information Integrity (SI) families.

Q11 Third-Party and Supply-Chain Risk

How do you manage cybersecurity risk introduced by your own vendors, suppliers, and sub-contractors?

- ☐ No supplier risk program.
- ☐ **Vendor questionnaires. At onboarding only.**
- ☐ **Vendor cybersecurity attestations. SOC 2, ISO 27001, or equivalent required.**
- ☐ **Flow-down of CMMC requirements. To all sub-contractors who touch CUI on your behalf.**
- ☐ **Supplier audit program. Active assessment of supplier security posture.**

How many of your sub-contractors or suppliers handle CUI on your behalf?

Why this matters: Primes are increasingly requiring sub-primes to flow CMMC requirements down to their own sub-tier. If you sub-contract any work involving CUI, those sub-contractors are part of your assessment narrative.

Q12 Incident Response Readiness

How prepared is your organization to detect, respond to, and report a cybersecurity incident?

- ☐ No incident response (IR) plan.
- ☐ **IR plan exists, But has not been tested.**
- ☐ **IR plan plus tabletop. With an annual tabletop exercise.**
- ☐ **IR plan plus tabletop plus retainer. With a qualified IR firm.**
- ☐ **IR plan plus tabletop plus retainer plus breach-notification automation. DFARS 7012 requires 72-hour reporting to DoD via DIBNet.**

Does your IR plan include the DFARS 252.204-7012 72-hour reporting requirement to dibnet.dod.mil?

- ☐ Yes
- ☐ No
- ☐ Unsure

Do you have an active DoD-approved External Certificate Authority (ECA) or DoD PKI certificate to submit DIBNet incident reports?

- ☐ Yes
- ☐ No
- ☐ Unsure

Why this matters: CMMC Level 2 requires a documented and tested IR plan plus the contractual reporting capability under DFARS 7012. The 72-hour clock is unforgiving. Organizations without DIBNet capability cannot satisfy the reporting requirement on their own.

Scoping Outcome (Self-Scoring)

Tally your answers across all 12 questions. The pattern you check most often suggests the engagement bracket. These brackets are typical project lengths from prior engagements, framed by length and not by dollars.

Your answer pattern	Likely engagement
Mostly first-listed answers, Level 1 contract, FCI only	**Level 1 Readiness, approximately 30 days**
Mixed mid-range answers, Level 2 contract, some gaps, no SSP or stale SSP	**Level 2 Gap Assessment, approximately 60 to 90 days**
Mostly mature answers, Level 2 contract, mature program	**Level 2 Full Readiness to C3PAO assessment, approximately 6 to 9 months**
Any Level 3 contract requirement	**Scope-dependent. Schedule a consultation for an engagement-length estimate.**

Your specific engagement length depends on enclave architecture decisions, current SSP maturity, headcount, and the number of in-scope systems.

> **Petronella Technology Group, Inc. does not publish fixed CMMC pricing. Custom-quote model only. The scope drives the price, and we will not quote without proper scoping.**

Schedule your free 30-minute scoping consultation

Phone: (919) 348-4912 **Web: https://petronellatech.com/contact-us/**

On the call we will:

1. Walk through your completed worksheet.
2. Confirm the data classification (FCI, CUI, CUI Specified).
3. Sketch a proposed scope of work.
4. Deliver a realistic engagement-length estimate.
5. Discuss the self-assessment versus C3PAO assessment decision.

We will not deliver a fixed price on the call. We will deliver a fixed price after scoping.

Next Steps After You Complete the Worksheet

- [ ] Save the completed worksheet (PDF or scan).
- [ ] Email the completed worksheet to your Petronella scoping coordinator with the subject line "CMMC Scoping Worksheet - [Your Company Name]".
- [ ] Schedule your free 30-minute scoping consultation at petronellatech.com/contact-us/ or call (919) 348-4912.
- [ ] Identify your call attendees: one decision-maker (owner, COO, or compliance lead) and one technical lead (CIO, IT director, or security lead).
- [ ] Have your DFARS-bearing contracts available during the call for clause-by-clause review.

What to expect on the scoping call

- 30 minutes, video or phone.
- A Petronella Technology Group CMMC-RP walks through your worksheet.
- Output: engagement-length estimate, proposed scope of work, and a decision aid for the self-assessment versus C3PAO path.
- No pricing pressure. No fixed quote on the call. The fixed quote follows scope confirmation.
- No obligation. If we are not the right fit, we will say so and recommend alternatives.

After the call

If you proceed, Petronella Technology Group, Inc. delivers a written scope of work with a fixed price, payment terms, and an engagement timeline. Engagements begin after contract execution. 100% payment is due at contract execution for all fixed-fee milestones.

About Petronella Technology Group, Inc.

Petronella Technology Group, Inc. is a CMMC-AB Registered Provider Organization helping Defense Industrial Base contractors scope, prepare for, and achieve CMMC certification across Levels 1, 2, and 3.

Certifications and registrations

- CMMC-AB Registered Provider Organization #1449. Verify our registration on the CyberAB Marketplace at cyberab.org/Marketplace.
- Entire team CMMC-RP certified: Craig Petronella, Blake Rea, Justin Summers, Jonathan Wood.
- Craig Petronella: CMMC-RP, Cisco Certified Network Associate (CCNA), Certified Wireless Network Expert (CWNE), Digital Forensic Examiner (DFE) #604180, MIT-Certified in AI and Blockchain.

Track record

- Better Business Bureau A+ rating since 2003.
- Founded 2002. More than two decades supporting regulated industries.
- Author of multiple cybersecurity titles.

Industries served

- Defense Industrial Base (sub-primes across Tier 1 and Tier 2)
- Healthcare and HIPAA-regulated organizations
- Engineering and architecture firms
- Legal and law firms
- Financial services

Prime contractor flow-downs

We support sub-primes inheriting CMMC flow-down requirements from major DoD prime contractors across the aerospace, defense electronics, and ground systems sectors.

Headquarters and service area

5540 Centerview Dr., Suite 200, Raleigh, NC 27606
Phone: (919) 348-4912 | Web: petronellatech.com
North Carolina headquartered with national remote engagement.