CMMC COMPLIANCE WORKBOOK SERIES

WORKBOOK 1

Am I In Scope?

CMMC Scope Determination & Triage Guide
for Small Defense Contractors

Applies To:	All DoD contractors and subcontractors
CMMC Levels Covered:	Level 1 and Level 2
Phase 1 Status:	ACTIVE — Effective November 10, 2025
Version:	1.0 • March 2026
Regulatory Basis:	32 CFR Part 170, FAR 52.204-21, 48 CFR Final Rule

■ LEGAL DISCLAIMER — READ BEFORE PROCEEDING

This workbook is an educational and self-assessment tool. It does not constitute legal advice, cybersecurity consulting, or a guarantee of CMMC compliance. False certifications submitted to DoD may expose organizations and senior officials to False Claims Act (FCA) liability, including damages up to three times the value of the affected contract. Consult qualified legal counsel before submitting any compliance certification to the DoD.

Time Required: Approximately 15–20 minutes | No technical background required

HOW TO USE THIS WORKBOOK

Purpose

This workbook helps you answer one critical question: **Which CMMC (Cybersecurity Maturity Model Certification) level applies to your business?** Your answer determines everything — which controls you must implement, what documentation you need, and how you certify compliance with the Department of Defense (DoD).

Work through this guide in order:

Step 1	Read the plain-English definitions of FCI and CUI (Sections 1–2).
Step 2	Review the real-world examples and "you might not realize" scenarios (Section 3).
Step 3	Complete the Decision Flowchart (Section 4) — this gives you your CMMC level.
Step 4	Review your CUI categories if applicable (Section 5).
Step 5	Read the enforcement timeline (Section 6) to understand your deadlines.
Step 6	Complete the Triage Output Form (Section 8) and proceed to the correct next workbook.

■ Also Complete the Excel Decision Tool

This workbook comes with a companion Excel file: "WB1_CMMC_Scope_Decision_Tool_v1.xlsx". Use the Excel tool alongside this guide — it walks you through Yes/No questions and automatically calculates your recommended CMMC level with a printed summary you can keep on file.

SECTION 1 | What Is Federal Contract Information (FCI)?

1.1 Official Definition

Official Definition — FAR 4.1901:

"Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public websites) or simple transactional information, such as necessary to process payments."

1.2 Plain-English Translation

FCI is **any information your business receives from or creates for the federal government as part of a government contract** — as long as it is not something the government already makes public. Think of it as "work product information" tied to a government job.

If your company has a federal contract of any kind — even a simple purchase order for goods or services — there is a strong chance you handle FCI. FCI is the baseline threshold. **Almost every DoD contractor handles FCI.**

1.3 Real-World FCI Examples for Small Contractors

Contractor Type	Example of FCI They Handle
Machine Shop / Manufacturer	Technical drawings, specifications, or statements of work received from a prime contractor or government agency describing parts to be made under a DoD contract.
Electrical / Construction Contractor	Project plans, site surveys, and contract documents related to work on a military base or government facility.
IT Services / MSP	Network diagrams, system configurations, and project documentation created while supporting a government contractor's IT environment.
Logistics / Trucking	Shipping manifests, delivery schedules, and cargo documentation tied to a government contract — even if the cargo itself is commercial goods.
Staffing Agency	Personnel placement records, labor categories, and billing information generated under a government staffing contract.
Professional Services	Reports, analyses, and deliverables created under a consulting contract with a federal agency or prime contractor.

■ Key Rule: FCI = CMMC Level 1 Minimum

If you handle FCI and NOTHING more sensitive, you need CMMC Level 1. Level 1 requires compliance with 15 basic cybersecurity practices from FAR clause 52.204-21. See Workbook 2 for the complete Level 1 guide.

SECTION 2 | What Is Controlled Unclassified Information (CUI)?

2.1 Official Definition

Official Definition — 32 CFR 2002.4(h):

"Controlled Unclassified Information means information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls."

2.2 Plain-English Translation

CUI is information that is **sensitive but not classified**. The government has determined it needs special handling — it cannot be freely shared, must be protected from unauthorized access, and in many cases cannot leave the country. CUI is more sensitive than basic FCI.

Unlike FCI, **CUI has specific category labels**. If you receive a document stamped "CUI," "CONTROLLED," or see a DFARS 252.204-7012 clause in your contract, you handle CUI. Handling CUI means you need **CMMC Level 2**.

2.3 Real-World CUI Examples for Small Contractors

CUI Category	What It Looks Like for a Small Contractor
Technical Data / ITAR	Engineering drawings, CAD files, test results, or specifications for defense systems, weapons, or controlled military technology. Often marked "ITAR" or "EAR."
Export Controlled (ECI)	Research, designs, or data subject to U.S. export control laws. Receiving this via email or file transfer means you handle CUI.
Contractor Bid & Proposal Info	Pricing data, cost estimates, or technical approaches submitted in response to a government solicitation.
Privacy / PII	Personally identifiable information about DoD personnel, veterans, or employees (names, SSNs, addresses, medical info) received in connection with a contract.
Operational / Mission Info	Schedules, deployment plans, or logistics data related to military operations or base activities — even if it seems routine.
Naval Nuclear Propulsion Info	Any data related to nuclear-powered vessels. Extremely sensitive; very few small contractors encounter this.
Law Enforcement / Investigation	Case files, subject information, or investigative documents received from federal law enforcement clients.

■ Key Rule: CUI = CMMC Level 2 Required

If you handle CUI — even a single document, email, or file — you need CMMC Level 2. Level 2 requires implementation of all 110 controls in NIST SP 800-171 Rev 2. This is a significantly larger undertaking than Level 1. Start Workbooks 2 through 6 now.

SECTION 3 | "You Might Think You Don't Handle CUI, But You Do If..."

Many small contractors underestimate their CMMC level because CUI can arrive in unexpected ways. Here are the most common scenarios where businesses discover they handle CUI:

Scenario: Your prime contractor sent you drawings or specs by email

Technical drawings for defense systems almost always contain CUI (Technical Data). The fact that they were emailed to you does not make them less sensitive. Your email server and any system where you store or open those files is now in scope for CUI handling.

Scenario: You do physical work on a base but "don't touch computers"

If you received any electronic plans, access codes, operational schedules, or personnel lists to do your job — that is CUI. The physical nature of your work does not change the classification of the information you needed to do it.

Scenario: You're a subcontractor to a prime, not a direct DoD vendor

CMMC requirements "flow down" to subcontractors. If the prime's contract includes a DFARS 252.204-7012 clause, they are required to pass those obligations to you when they give you CUI or FCI. Your contract with the prime may already include this language.

Scenario: Your contract is small — under $250,000

There is no dollar threshold exemption in CMMC. A $50,000 subcontract that involves CUI requires the same Level 2 compliance as a $50 million prime contract.

Scenario: You use a cloud service or MSP to handle your data

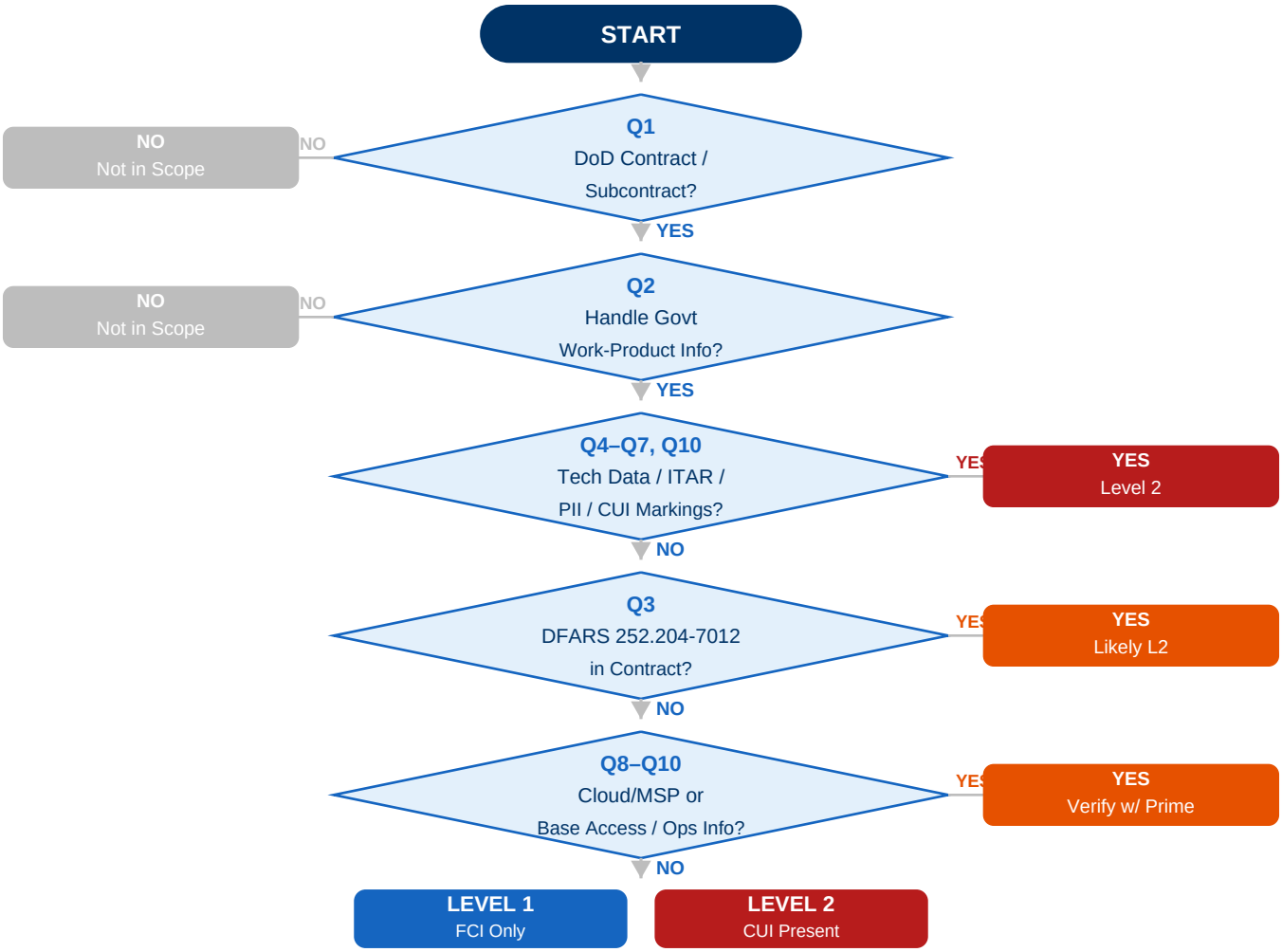
Using a cloud service (like Microsoft 365, Google Workspace, or a third-party IT provider) does not move CUI out of your scope. YOU remain responsible for ensuring those systems meet CMMC requirements. Your cloud environment IS your system boundary.

Scenario: The contract doesn't explicitly say "CUI"

Not all CUI is labeled correctly. If you receive technical specifications, personnel data, or operational information under a DoD contract, it may be CUI regardless of labeling. When in doubt, ask your contracting officer or the prime contractor in writing.

SECTION 4 | CMMC Level Decision Flowchart

Use the flowchart below to determine your CMMC level. Each decision point references the full verbatim question in the table that follows. Follow the arrows — exit on the first branch that applies to you.



Refer to table below for full details.

Q#	Topic	Full Question Text	Decision Rule
Q1	**DoD Contract / Subcontract**	Does your business have any contract, subcontract, or agreement with the U.S. Department of Defense (DoD), OR with a prime contractor working on a DoD program?	*NO → CMMC does not apply. Stop here. | YES → Continue to Q2.*

Q2	**Handle Government Work-Product Information**	Does any of your DoD-related work involve receiving, storing, creating, or transmitting information for the government — beyond purely public information or simple payment processing?	*NO → Not in scope. | YES → You handle FCI. Level 1 minimum. Continue to Q3.*
Q3	**DFARS 252.204-7012 Clause**	Does your contract include the clause DFARS 252.204-7012 ("Safeguarding Covered Defense Information and Cyber Incident Reporting")?	*YES → Almost certainly handle CUI. Continue to Q4. | NO/Unknown → Continue to Q4.*
Q4	**Technical Drawings / Defense Specs**	Do you receive, store, process, or transmit technical drawings or specifications for defense systems, weapons, or controlled military equipment?	*YES → You handle CUI. Level 2 required. | NO → Continue to Q5.*
Q5	**Export-Controlled Data (ITAR/EAR)**	Do you handle data subject to export control laws — labeled ITAR (International Traffic in Arms Regulations) or EAR (Export Administration Regulations)?	*YES → You handle CUI. Level 2 required. | NO → Continue to Q6.*
Q6	**Personally Identifiable Information (PII)**	Do you receive or store personally identifiable information (PII) about DoD personnel, veterans, or government employees?	*YES → You handle CUI. Level 2 required. | NO → Continue to Q7.*
Q7	**CUI / CONTROLLED Markings**	Have you received any documents, files, or emails labeled "CUI," "CONTROLLED," or "FOUO" (For Official Use Only)?	*YES → You handle CUI. Level 2 required. | NO → Continue to Q8.*
Q8	**Cloud Services or MSP**	Do you use a cloud service or a Managed Service Provider (MSP) to store or process any information related to your DoD contracts? (Example MSP: a local IT company that manages your computers, email, firewall, and helpdesk for a monthly fee.)	*YES → Note: cloud/MSP systems are part of your compliance boundary. | Continue to Q9.*
Q9	**Prime or Subcontractor Relationship**	Are you a subcontractor to a prime contractor on a DoD program (rather than a direct DoD vendor)?	*YES → Check your subcontract for DFARS 252.204-7012 flowdown language.*
Q10	**Operational / Base Access Information**	Have you received any operational information, mission schedules, base access details, or similar data as part of performing work on or near a military installation?	*YES → You likely handle CUI. Level 2 required. | NO → Level 1 if only FCI.*

■ Not Sure? Default to Level 2

If you are genuinely uncertain whether you handle CUI, treat yourself as Level 2 and work through the full assessment. It is far better to over-prepare than to submit a false Level 1 certification and face False Claims Act exposure. When in doubt, consult your prime contractor or contracting officer in writing.

SECTION 5 | The Three CMMC Levels — What Each Requires

Source: 32 CFR Part 170. The CMMC program has three levels, each building on the previous.

Level 1 — Foundational

Who It Applies To	Contractors that handle Federal Contract Information (FCI) — the baseline for any DoD contractor.
What Is Required	15 cybersecurity practices drawn verbatim from FAR clause 52.204-21. These are basic, common-sense protections: control who can log into your systems, use antivirus software, control physical access, protect your network.
How You Certify	Annual self-assessment submitted to SPRS (Supplier Performance Risk System). You also submit an annual affirmation signed by a senior company official. No third-party assessor is required.
POA&Ms; Allowed?	NO. All 15 controls must be fully implemented before you submit. There is no grace period.

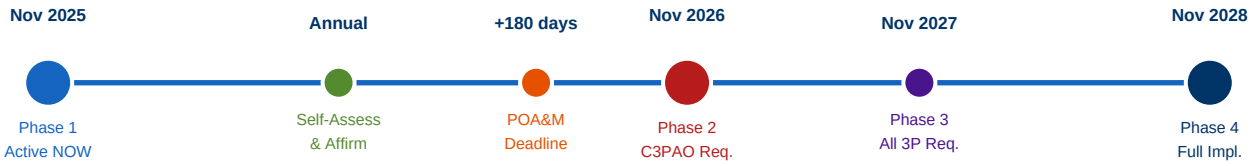
Level 2 — Advanced

Who It Applies To	Contractors that handle Controlled Unclassified Information (CUI) — more sensitive than FCI.
What Is Required	110 cybersecurity practices from NIST SP 800-171 Rev 2, organized into 14 control families. These include advanced requirements like multi-factor authentication (MFA), system security plans, incident response procedures, and audit logging.
How You Certify	Either a self-assessment or a third-party (C3PAO) assessment, depending on the contract. Phase 1 (active now) allows self-assessment for most contracts. Phase 2 (November 2026) will require C3PAO certification for many CUI contracts.
POA&Ms; Allowed?	YES — but with limits. You may have open items (gaps) when you submit, but ALL POA&M; items must be closed within 180 days of receiving Conditional CMMC Status.

Note: CMMC Level 3 exists for contractors handling the most sensitive CUI on critical DoD programs. Level 3 requires a government-led assessment and 24 additional controls beyond Level 2. Very few small businesses will need Level 3. This workbook series covers Levels 1 and 2 only.

SECTION 6 | Enforcement Timeline — Key Dates You Must Know

All dates sourced from: 48 CFR Final Rule (Federal Register, September 10, 2025) and 32 CFR Part 170.



6A | Government Enforcement Dates

These are the mandatory dates set by the DoD in the 48 CFR Final Rule. They apply to ALL contractors in scope and are tied to new contract solicitations.

November 10, 2025	PHASE 1 — ACTIVE NOW
CMMC Level 1 and Level 2 self-assessments required in all new DoD solicitations. Contractors without a submitted self-assessment and affirmation in SPRS may be ineligible for new DoD contract awards. **This phase is currently active.**	

November 10, 2026	PHASE 2
Level 2 C3PAO (third-party assessor) certification required in most new solicitations involving CUI. Self-assessment alone will no longer be sufficient for many Level 2 contracts. Level 3 assessments begin for high-priority programs. **Less than 8 months away — begin preparation now.**	

November 10, 2027	PHASE 3
All applicable new contracts must include Level 2 or Level 3 third-party assessments as award conditions. The window for self-assessment-only compliance narrows significantly.	

November 10, 2028	PHASE 4 — FULL IMPLEMENTATION
CMMC fully implemented across ALL applicable DoD contracts including option periods. No waivers, no grace periods, no exceptions.	

6B | Recurring Compliance Obligations

These obligations repeat on an ongoing basis once you are certified. Missing them causes your certification to lapse, making you ineligible for contract awards until reinstated.

■ Level 1 — Annual Self-Assessment

Every 12 months, you must re-complete your Level 1 self-assessment and re-submit your score in SPRS. This confirms that all 15 controls remain fully implemented.

■ Level 1 — Annual Affirmation

A senior official (e.g., owner, CEO, or authorized representative) must submit an annual affirmation in SPRS confirming that the self-assessment is accurate and the company remains compliant.

■ Level 2 — Annual Affirmation

Level 2 contractors must submit an annual affirmation in SPRS. Note: the full 110-control re-assessment is not required annually — but the affirmation confirming ongoing compliance is.

■ All Levels — Contract Change Review

Whenever you take on a new DoD contract or subcontract, re-evaluate your scope. New contracts may introduce CUI obligations that change your required CMMC level.

6C | Conditional Status & the 180-Day POA&M Deadline

Who this applies to: Level 2 contractors ONLY. This does not apply to Level 1.

When a Level 2 contractor submits a self-assessment to SPRS with one or more unimplemented controls, they may receive a **Conditional CMMC Status** rather than a full certification. This is not a failure — it is a temporary status that allows contract award while you finish closing your remaining gaps.

What is a POA&M;?

A Plan of Action & Milestones (POA&M;) is a documented list of controls you have not yet fully implemented, along with your plan and timeline for closing each gap. Each item must include: the control ID, description of the gap, planned corrective action, responsible party, resources required, and scheduled completion date.

What is the 180-Day Deadline?

Once you receive Conditional CMMC Status, ALL open POA&M; items must be closed — meaning every listed control must be fully implemented — within 180 days. If items remain open after 180 days, your Conditional Status lapses and you are no longer certified.

What Happens if You Miss the Deadline?

Your CMMC certification lapses. You will be unable to receive new DoD contract awards requiring CMMC Level 2 until you re-submit a compliant assessment. You may also face scrutiny regarding the accuracy of your original affirmation.

POA&M; at Level 1?

POA&Ms; are NOT permitted at Level 1. All 15 controls must be fully implemented before you submit your Level 1 self-assessment. There is no conditional status option for Level 1.

SECTION 7 | Common CUI Categories in Small Contractor Environments

CUI is organized into over 20 categories by the National Archives CUI Registry. The categories below are the most commonly encountered by small defense contractors. If you handle information in any of these categories, you handle CUI and need Level 2.

CUI Category	What This Means for Your Business
Critical Infrastructure	Information about systems and assets that, if compromised, would have a debilitating effect on security, the economy, or public health.
Defense / Technical Data	Engineering drawings, specifications, test results, and technical documentation related to defense systems or controlled items.
Export Controlled (EAR / ITAR)	Data subject to U.S. export control laws. Common in manufacturing, aerospace, and electronics sectors.
Financial (Government)	Budget data, cost or pricing data, and financial plans tied to government programs.
Intelligence	Information related to national intelligence activities. Rarely encountered by small contractors.
Law Enforcement	Investigative case files, subject data, or sensitive operational information from law enforcement agencies.
Legal	Privileged legal communications or pre-decisional legal documents.
Nuclear (Non-Weapons)	Data related to civilian nuclear operations. Rarely encountered by most small contractors.
Privacy / PII	Personally identifiable information about individuals — names, SSNs, medical info, financial data about people.
Procurement & Acquisition	Source selection information, bid/proposal data, contractor performance evaluations.
Proprietary Business Info	Sensitive commercial or financial data provided by contractors to the government.
Statistical	Pre-publication statistical data from federal agencies.
Tax	Federal tax return information or related financial data.
Transportation	Sensitive transportation security plans or infrastructure data.

For the complete list of CUI categories and their specific safeguarding requirements, visit the National Archives CUI Registry at: archives.gov/cui

SECTION 8 | Triage Output Form — Complete and Keep on File

Complete this form after working through Sections 1–7. Keep this completed form with your compliance documentation. You may also print the Results Summary from the companion Excel tool as an alternative record.

Company / Business Name	■ *enter here*
CAGE Code	■ *enter here*
Completed By (Name / Title)	■ *enter here*
Date Completed	■ *enter here*
Contract / Solicitation No. (if known)	■ *enter here*

Step 1 — Do you handle FCI?

■ YES — I have a DoD contract and handle work-product information for the government.

■ NO — I do not have any DoD contracts or subcontracts.

Step 2 — Do you handle CUI?

■ YES — My contract includes DFARS 252.204-7012 and/or I receive technical data, export-controlled information, personnel data, or other CUI.

■ NO — I only handle basic FCI; no CUI indicators are present in my contracts.

■ UNSURE — I am not certain. I will default to Level 2 and consult my prime contractor or contracting officer.

MY REQUIRED CMMC LEVEL IS:

■ CMMC LEVEL 1 I handle FCI only. No CUI present. → Proceed to Workbook 2: Level 1 Compliance Workbook	**■ CMMC LEVEL 2** I handle CUI (and FCI). → Proceed to Workbooks 2–6 (Levels 1 + 2)

Additional Notes / CUI Categories Identified:

This completed triage form should be retained as documentation for your CMMC compliance file. It does not substitute for a formal assessment. Re-evaluate annually or whenever your contracts change.