CMMC Requirements (Impact on Sales & Compliance)

A practical explainer for revenue, leadership, and capture teams

Disclaimer: This document is for general awareness only and is not legal advice or a substitute for guidance from your security, contracts, or legal teams.

1. WHY CMMC MATTERS TO REVENUE

The Cybersecurity Maturity Model Certification (CMMC) is now baked into how the Department of Defense (DoD) buys from industry. If your company cannot meet the CMMC level specified in a solicitation or contract, you may simply be ineligible to bid or win.

For sales and leadership teams, this means CMMC is no longer just an IT project. It is a go/no-go gate for a large portion of the defense market. CMMC affects:

- Which deals you are allowed to pursue.
- Whether you can be on a winning team as a prime or a subcontractor.
- The risk that a contract award is protested, terminated, or questioned in an audit.
- Your reputation with government customers as a trustworthy steward of their data.

If you sell into the defense market, you need a basic working vocabulary for CMMC so you can:

- Qualify opportunities correctly.
- Coordinate with your security and compliance teams.
- Talk credibly with customers about where you are today and where you are headed.

2. CMMC IN PLAIN LANGUAGE

CMMC is a DoD program that ties the sensitivity of information in a contract to specific cybersecurity practices and an assessment of how well those practices are implemented.

Key ideas in simple terms:

- Federal Contract Information (FCI)

Basic information provided by or generated for the Government that is not intended for public release. This typically requires CMMC Level 1 protections.

- Controlled Unclassified Information (CUI)

More sensitive unclassified information (for example, design details, technical data, or certain personnel and logistics data). CUI typically requires CMMC Level 2 or Level 3 protections.

- CMMC Levels

CMMC 2.0 uses three maturity levels:

* Level 1 – Foundational: Focused on basic cyber hygiene for FCI.

* Level 2 – Advanced: Based on the NIST SP 800-171 security requirements for protecting CUI.

* Level 3 – Expert: For the most sensitive programs, aligned with a subset of NIST SP 800-172.

- Assessment types

Depending on the contract, your company may need:

* A self-assessment with an annual affirmation.

* A third-party assessment by a Certified Third Party Assessment Organization (C3PAO).

* A government assessment for the highest level.

The required level and assessment type are specified by the Government for each contract. You do not get to pick your own level for a given opportunity.

3. HOW CMMC SHOWS UP IN REAL OPPORTUNITIES

From a sales and capture perspective, CMMC appears in three main places:

1) Pre-solicitation and market research

- Requests for information (RFIs), industry days, and draft solicitations may describe the type of data involved (FCI or CUI) and the expected CMMC level.
- Your job is to surface those early signals so security and leadership can judge whether the opportunity fits your current and planned posture.

2) Solicitations (RFPs, RFQs, BAAs, OTAs with CMMC language)

- DoD solicitations now include clauses that identify:

* The required CMMC level (1, 2, or 3).

* The assessment type (self, C3PAO, or government assessment).

* Any timing requirements, such as needing a current assessment before award or before exercising an option.

- Contracting officers will verify your status in DoD systems such as the Supplier Performance Risk System (SPRS), not just take your word for it.

3) Contract administration and performance

- Maintaining your CMMC status is not a “one-and-done” event.
- You must continue to meet the required practices, update scores and affirmations on schedule, and ensure that any systems used on the contract remain within the assessed scope.
- Significant changes (for example, moving to a new cloud environment) can require updates to your assessment and documentation.

From a revenue lens: a contract is only secure if your CMMC posture stays aligned with what the contract demands over time.

4. WHAT SALES TEAMS SPECIFICALLY NEED TO KNOW

You do not need to be a security engineer, but you do need to understand how CMMC affects pursuit decisions, teaming, and conversations with customers.

A. Opportunity qualification questions

For every defense opportunity, your sales or capture team should be able to answer:

1) What data will we handle?

- Only FCI?
- Any CUI? If so, what kind?
- Will we host, process, or transmit that data on our own networks or cloud environments?

2) What CMMC level and assessment type are required?

- Is this a Level 1 self-assessment, a Level 2 third-party certification, or something else?
- Is there a deadline by which the level must be in place (for example, before award, before option year, or within a certain number of days)?

3) Where are we today?

- What CMMC level and scope does our organization currently support?
- Are we working under a conditional or in-progress plan to close remaining gaps?
- Who is our internal “affirming official” or compliance owner?

4) Can we credibly meet the requirement on time?

- If we are not yet at the required level, is there a realistic plan to get there before the customer needs proof?
- Have we coordinated with security, IT, contracts, and leadership about this specific pursuit?

If you cannot get clear answers to these questions, you are flying blind on CMMC risk for that deal.

"Area Intentionally Left Blank"

B. Teaming and subcontractor risk

Even if your own company is ready, your partners might not be. Sales and capture teams must:

- Confirm that teammates who will handle FCI or CUI understand the required CMMC level.
- Ensure that primes and subs know who is responsible for which systems and environments.
- Recognize that a non-compliant subcontractor can jeopardize the entire team’s eligibility and schedule.

C. How to talk with customers about CMMC

Good practices:

- Be honest about your current status and roadmap.
- Emphasize your governance model (for example, who owns cyber compliance, how often you review posture, how you manage subcontractors).
- Use plain language: explain how you protect their data and how CMMC assessments back that up.

Bad practices:

- Promising a CMMC level you have not achieved or scoped.
- Dismissing CMMC questions as “something IT handles.”
- Using vague phrases like “we are compliant” without being able to explain what that means in practice.

5. WHAT LEADERSHIP NEEDS TO UNDERSTAND

A. CMMC is a revenue strategy decision

CMMC investment is about choosing which part of the defense market you want to compete in.

- Staying at Level 1 may be cheaper but limits you largely to work with only FCI.
- Investing to reach Level 2 (and eventually Level 3, if needed) opens access to a much broader set of contracts that involve CUI.
- Your company’s risk appetite and growth targets should drive a clear, documented CMMC strategy.

B. Accountability and governance

Executives must ensure that:

- There is a named executive owner for CMMC and related DFARS cybersecurity clauses.
- The “affirming official” understands that inaccurate representations can create False Claims Act and suspension/debarment risk.
- Cybersecurity, contracts, capture, and operations regularly share information about upcoming opportunities and the environments needed to deliver them.

C. Budgeting and prioritization

Leadership decisions directly affect how quickly the company can reach and maintain the required CMMC levels. Key levers include:

- Funding for security tools, secure enclaves, and compliant cloud environments.
- Staffing for cybersecurity, compliance documentation, and assessment preparation.
- Training for sales, program managers, and technical leads on handling CUI and using approved environments.

D. Supply chain and partner management

Prime contractors carry responsibility for ensuring that subcontractors who handle FCI or CUI meet applicable CMMC requirements. Leadership should:

- Establish minimum cybersecurity expectations for partners.
- Decide which types of work can be sourced only to partners with verified CMMC status.
- Build processes to collect and track partner attestations or certifications.

6. PRACTICAL CHECKLIST FOR PURSUITS

This checklist is designed for capture managers and account teams working with security and contracts.

Before you commit resources to a pursuit:

1) Confirm the expected CMMC level and assessment type.

2) Validate what kinds of information will flow to your systems (FCI only, or CUI as well).

3) Verify your current CMMC status and scope with the internal compliance owner.

4) Check whether key partners on the team will need their own CMMC status.

When the solicitation drops:

5) Read all CMMC and cybersecurity clauses carefully; note any timing or reporting obligations.
6) Confirm that your CMMC status in SPRS (or other government systems) lines up with what the solicitation expects.
7) Factor any required upgrades or assessments into your bid/no-bid decision and price/capture strategy.

After award:

8) Make sure program managers know which systems are in scope for the contract's CMMC level.
9) Coordinate any significant changes (for example, new hosting locations, major architecture changes, or new subcontractors) with your security and contracts teams before implementation.
10) Track upcoming re-assessment or affirmation deadlines as part of standard contract management.

Area Intentionally Left Blank

7. TALKING POINTS FOR NON-TECHNICAL EXECUTIVES

Use or adapt these short statements when communicating with customers, partners, and internal stakeholders.

- “We treat your data as a core part of the mission. CMMC helps prove that our cybersecurity practices match the sensitivity of the information you entrust to us.”

- “For each opportunity, we map the type of data and required CMMC level to specific systems and controls, so we only bid work we can deliver securely and compliantly.”

- “Our leadership team reviews our CMMC posture regularly. We have a named executive owner and an
affirming official who is accountable for the accuracy of our representations to DoD.”

- “We work closely with our partners and subcontractors to make sure that anyone handling Federal Contract Information or Controlled Unclassified Information meets the appropriate requirements.”

- “CMMC is not just a compliance checkbox for us; it is part of how we protect national security information and earn the trust of our government customers.”

8. WHAT TO DO NEXT

If you are in sales, capture, or leadership, you do not need to memorize every control in CMMC. You do need to:

- Know your company’s current and target CMMC level.
- Build CMMC questions into your opportunity qualification and teaming discussions.
- Loop in your security, compliance, and legal experts early when new opportunities involve CUI or higher-risk data.
- Treat CMMC status as a core part of your revenue planning, just like pricing, past performance, or key personnel.

When your teams understand CMMC at this practical level, you reduce surprise “showstoppers,” protect existing contracts, and position your company as a reliable, low-risk partner for the Department of Defense