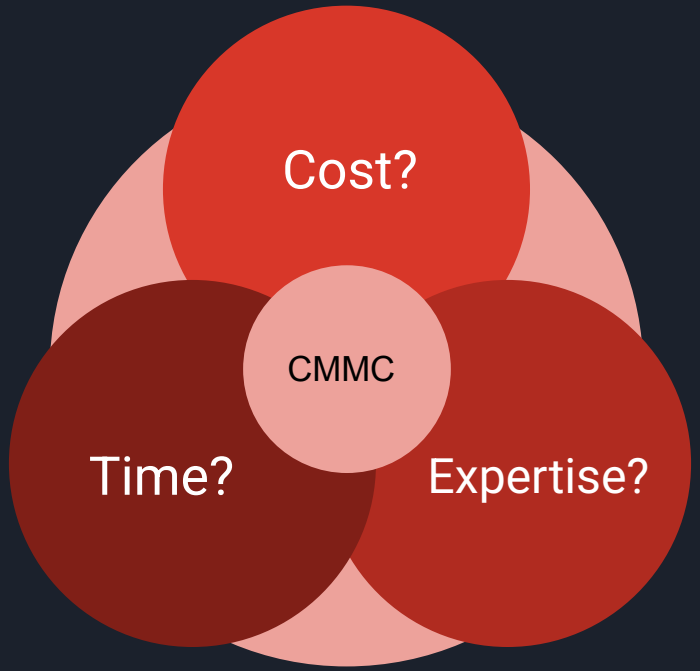
CMMC Level 1 Compliance Overview

NC STATE UNIVERSITY

Industry Extension Services

IES Presents: Streamlining CMMC Compliance Series, Part 1

Our Goal Today: Make CMMC Easy to Understand and Easier to Achieve



The Who, What, When, & Why of CMMC

Our Learning Objective Today is Solving The CMMC FAQs

- What is CMMC?
- Do we really need to comply?
- How to I get started?
- Why does it cost so much?
- What level is required?
- Where do I submit my CMMC info?
- When do I need to be ready?

The Who, Key CMMC Roles: The CMMC Ecosystem Pt.1

- **Department of Defense (DoD):** Responsible for developing and mandating the CMMC framework as a cybersecurity requirement for its contractors and suppliers
- **Cyber Accreditation Body (Cyber-AB):** Nonprofit organization authorized by the DoD to oversee the training, accreditation, and certification of CMMC assessors and organizations seeking CMMC certification
- **CMMC Certified Assessors:** CMMC assessors are qualified individuals or organizations authorized by The Cyber AB to evaluate and assess organizations against the CMMC framework. They conduct on-site or remote assessments to determine if an organization meets the required cybersecurity practices and processes for certification

Key CMMC Roles: The CMMC Ecosystem Pt.2

- **CMMC Third-Party Assessment Organizations (C3PAOs):** C3PAOs are organizations authorized by The Cyber AB to perform official CMMC assessments. They employ CMMC assessors and are responsible for conducting the assessments and issuing CMMC certifications to organizations that meet the requirements
- **CMMC Practitioners:** CMMC practitioners are individuals with deep knowledge and practical experience in cybersecurity and the CMMC framework. They provide guidance and support to organizations throughout their CMMC journey, helping them build robust security programs
- **Defense Contractors and Suppliers:** Referred to as OSA (Organizations Seeking Assessment), These are the organizations that work with the DoD and are subject to CMMC requirements. They must implement the necessary cybersecurity controls, practices, and processes to achieve certification and maintain compliance with the appropriate CMMC level

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is the DoD's (DoW) requirement for small businesses who are in the Defense Industrial Base (DIB). In easier terms, if you do business with the DoD as a prime or subcontractor you are most likely required to comply

Who Must Comply?

More than 220,000 defense contractors and subcontractors

When Does it Start?

3 year phased rollout began 11/10/25. In select contracts today

What is the Goal?

Contractors must meet minimum security requirements to work with federal government

The When: CMMC Implementation Timeline

PHASE 1

Begins 10 Nov 2025

Self-assessments for Level 1 or 2 required in applicable solicitations

PHASE 2

Begins 10 Nov 2026

Level 2 C3PAO assessment required for CMMC Level 2 (no more self-assessment). Department may delay to option periods

PHASE 3

Begins 10 Nov 2027

Level 3 Certification required for applicable solicitations. Widespread rollout of CMMC in new solicitations

PHASE 4

Begins 10 Nov 2028

Full Implementation: All solicitations include CMMC requirements

By 2028, every contractor processing FCI or CUI must maintain an active CMMC certification or self-assessment in SPRS

How Does it Work? CMMC Levels Explained

LEVEL 1
FOUNDATIONAL

SELF-ASSESS

Focus: Basic Cyber Hygiene

Requirements:
17 basic safeguarding requirements aligned with FAR 52.204-21

Who:
Contractors handling Federal Contract Information (FCI)

Assessment:
Annual self-assessment

LEVEL 2
ADVANCED

MOST COMMON

Focus: Protecting CUI

Requirements:
110 security requirements aligned with NIST SP 800-171

Who:
Contractors handling Controlled Unclassified Information (CUI)

Assessment:
Third-party audit by C3PAO (or self-assessment for lower priority)

LEVEL 3
EXPERT

HIGHEST RISK

Focus: High-Value CUI

Requirements:
130+ requirements including NIST SP 800-172 enhancements

Who:
Contractors on the most sensitive DoD programs

Assessment:
Government-led DIBCAC assessment

Phase 1: Self-assessments (Now) → Phase 2: C3PAO audits (Nov 2026) → Phase 3: Level 3 enforcement (Nov 2027) → Phase 4: Full rollout (Nov 2028)

So What CMMC Level is My Business?

✅ CMMC LEVEL 1

Federal Contract Information (FCI)

Sensitive, but not classified, information that is provided by or generated for the government under a contract

Not intended for public release

Examples: *Contract details, building specs not on SAM, project schedules, CO communications, organizational charts, process documentation, contract performance reports, RFP or RFI responses*

✅ CMMC LEVEL 2

Controlled Unclassified Information

Sensitive information, while unclassified, that requires safeguarding and dissemination of security controls pursuant to federal laws, regulations, and policies

(SHOULD) Be marked CUI

Examples: *Engineering drawings, SSNs, financial data, trade secrets, applicant data, Proprietary Business Information (PBI), Unclassified Controlled Technical Information (UCTI), Sensitive but Unclassified (SBU), For Official Use Only (FOUO), Law Enforcement Sensitive (LES)*

How to Scope for CMMC Level 1

Clearly define your Assessment Scope before starting self-assessment

Process

Systems using FCI in some way

- Editing
- Generating
- Printing

Store

Systems keeping FCI at rest

- Server files
- Computer storage
- Paper records

Transmit

Systems moving FCI

- Email
- Uploads
- File transfers

*If an asset touches FCI in any of these ways, **it's in scope**.*

CMMC Level 1 Scoping Guide

Essential Reading: Use the DoD's 8-page Scoping Guide!

Analyze your FCI Data Flow:

- What specific devices (referred to as assets) handle FCI?
- Are all assets that touch FCI located on premises?
- Is any FCI stored in a cloud environment?
- Is FCI on physical media (flash drives, printed materials)?
- Who exactly handles and accesses this FCI?

Clearly define your Assessment Scope before starting your self-assessment

CMMC Level 1: Foundational

15
Security Practices

6
Practice Domains

SELF
Assessment Type

Six Security Domains (AKA Control Families)

- Access Control (AC)
- Identification & Authentication (IA)
- Media Protection (MP)
- Physical Protection (PE)
- System Communications Protection (SC)
- System & Information Integrity (SI)

POA&Ms not permitted for Level 1

So What Do I Actually Do for CMMC Level 1?

Access Control & Identity

- Limit system access to authorized users, processes, or devices
- Restrict transactions and functions to permitted user roles
- Verify and control connections to external information systems
- Control info posted on publicly accessible systems
- Identify and authenticate users/devices as a prerequisite for access

Physical & Media Security

- Sanitize/destroy media containing FCI before disposal or reuse
- Limit physical access to systems and equipment to authorized staff
- Escort visitors and monitor their activity; maintain logs
- Manage physical access devices and boundary controls

System Information & Integrity

- Implement subnetworks to separate public components from internal networks
- Identify, report, and correct system flaws in a timely manner
- Protect systems from malicious code at appropriate locations
- Update protection mechanisms when new releases are available
- Perform periodic and real-time scans of files from external sources

CMMC Level 1 focuses on basic safeguarding of FCI (Federal Contract Information)

CMMC Level 2: Advanced

110
Security Practices

14
Practice Domains

SELF (in phase 1),
C3PAO (optional in phase 1)
Assessment Type

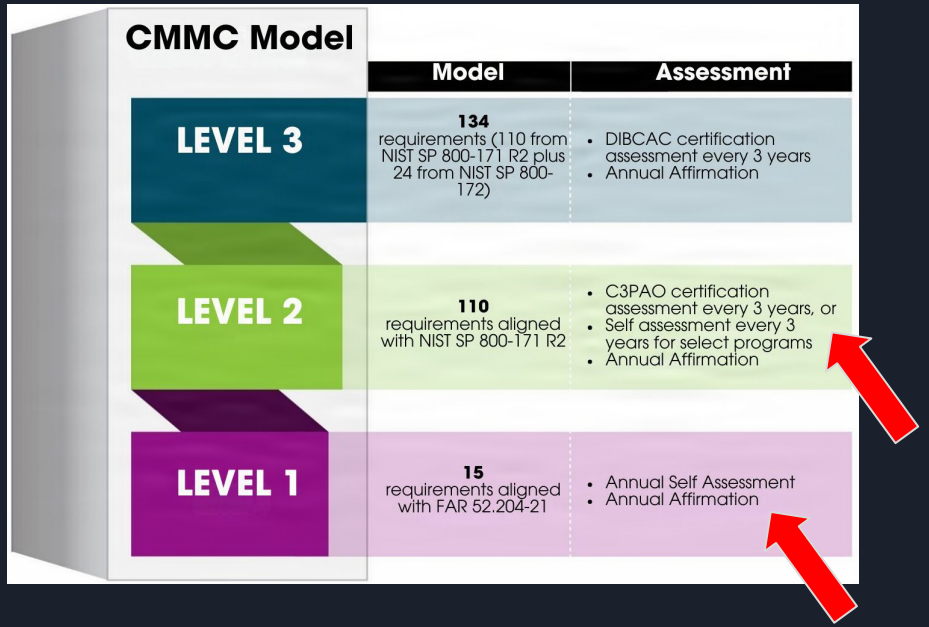
Fourteen Security Domains (AKA Control Families)

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)
- System Communications Protection (SC)
- System & Information Integrity (SI)

Limited, specific use of POA&Ms permitted for Level 2. 180 day close out required

Are CMMC Assessments an Annual Requirement?

- CMMC Level 1: Self Assessment, Annual Affirmation required
- CMMC Level 2: Self (in Phase 1) or Third Party (C3PAO) Assessment every 3 years, with Annual Affirmation
- If major changes have occurred (new facility, company merger, major process change involving FCI or CUI, etc.) new assessment is required



CMMC Level 1 Self-Assessment Guide

Essential Reading: Use the DoD's 54 page Assessment Guide!

Analyze your Current FCI protection:

- Review each assessment objective, 59 in total
- Document the policies, procedures, and security plans you have in place to protect FCI and meet assessment objectives
- Test policies and procedures to ensure they are in place, document
- Aim to accomplish the assessment objectives in the most cost-effective manner possible
- Observe safeguards are in place by viewing hardware, associated configuration information, or observing staff following a process

All objectives must be MET for successful completion, this is a point in time assessment!!

Reviewing an Assessment Objective

Access Control (AC)

AC.L1-B.1.I – AUTHORIZED ACCESS CONTROL [FCI DATA]

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A][3]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A][3]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan[45]; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Implementation Example

A coworker wants to add a new multi-function printer to the network.

You explain that the company controls system and device access, preventing unauthorized access.

You help the coworker submit a ticket that asks for the printer to be granted access to the network, and appropriate leadership approves the device.

- Assessment Consideration: **Is a list of authorized users/devices maintained that defines their identities and roles?**

Reference: NIST SP 800-171A Assessment Objectives

Barriers to Success

Internal Human Resources
Staff capability for regulatory requirements and CMMC implementation

Limited Time
Availability of current staff to manage and handle new, complex tasks

Marketplace Capacity
Limited number of qualified CMMC assessors and C3PAOs service providers

Cost & Resources
Labor, Software, Hardware
Ongoing license/hosting fees

Documentation: Creating Evidence

Most small businesses have little or no formal documentation

You may be meeting many of the requirements of CMMC today, but have no ability to audit these processes because of lack of documentation

Proactive Recording

Record everything you can about the current status of your organization's cybersecurity program. This will help populate your System Security Plan (SSP)

Core Documentation Artifacts

SSP

The core of your documentation. Includes system boundaries, environments of operation, and security requirement fulfillment

Policies and Procedures

High-level guidelines (Policies) and granular, step-by-step instructions (SOPs) for team execution

POA&M**

Outlines steps, resources, and timelines to correct deficiencies identified during gap assessments. *It may be helpful for internal use, but not part of the final CMMC submission process at Level 1!*

Network & Data Flow Diagrams

Critical for visualizing FCI/CUI storage and transmission, and defining data ownership scope

***Remember that CMMC Level 1 does not permit POA&M*

Remember Annual Affirmation

- The CMMC Annual Affirmation is a mandatory yearly requirement under 32 CFR 170.22 where a senior company executive (the "Affirming Official") formally attests in the Supplier Performance Risk System (SPRS) that their organization continuously maintains its Cybersecurity Maturity Model Certification
- Don’t wait until deadline to start this process, cyber programs are ongoing and rely on on continuous monitoring and updates to policy, procedure, and documentation

Major Changes to Environment

Requirement: A new assessment is required if there are significant architectural or boundary changes to the previous CMMC Assessment Scope

Note: Operational changes within an existing boundary following the SSP (like adding/subtracting resources) do not require a new assessment, but are covered by annual affirmations

Examples Requiring New Scope/Assessment

New facility

New cloud provider/environment

Major technology upgrades

Cyber Security Awareness & Training

CMMC Requirement: Level 2 requires cyber awareness and training for all relevant personnel

Key Benefits

- Reduce chances of expensive breaches
- Improve customer confidence
- Differentiate from competitors
- Lessen impact of incidents
- High ROI vs cost of breach

The Human Factor

Humans are involved in most breaches. Focus on **people** more than systems

Ongoing Commitment

Train at hire, annually, and maintain regular discussions in monthly meetings

* All companies should maintain basic awareness training regardless of specific regulatory requirements

Resources

DoD CMMC Website
Official CMMC information and policy updates, CMMC marketplace

https://dodcio.defense.gov/CMMC/

Lynx
Unified platform for opportunities and status

https://www.lynxconnect.io/

Project Spectrum
Cyber readiness for the defense supply chain

https://www.projectspectrum.io/

SPRS
Required entry for CMMC compliance

https://www.sprs.csd.disa.mil/

CUI Training
Mandatory training for handling CUI

https://securityawareness.dcsa.mil/cui/index.html

IES Cyber
NCSU resources for small business security

https://ies.ncsu.edu/cybersecurity/