CMMC Level 1- Part 2, Getting Started

NC STATE UNIVERSITY

Industry Extension Services

IES Presents: Streamlining CMMC Compliance Series, Part 2

Getting Started with CMMC- Scoping, Policy Creation, & Assessment

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

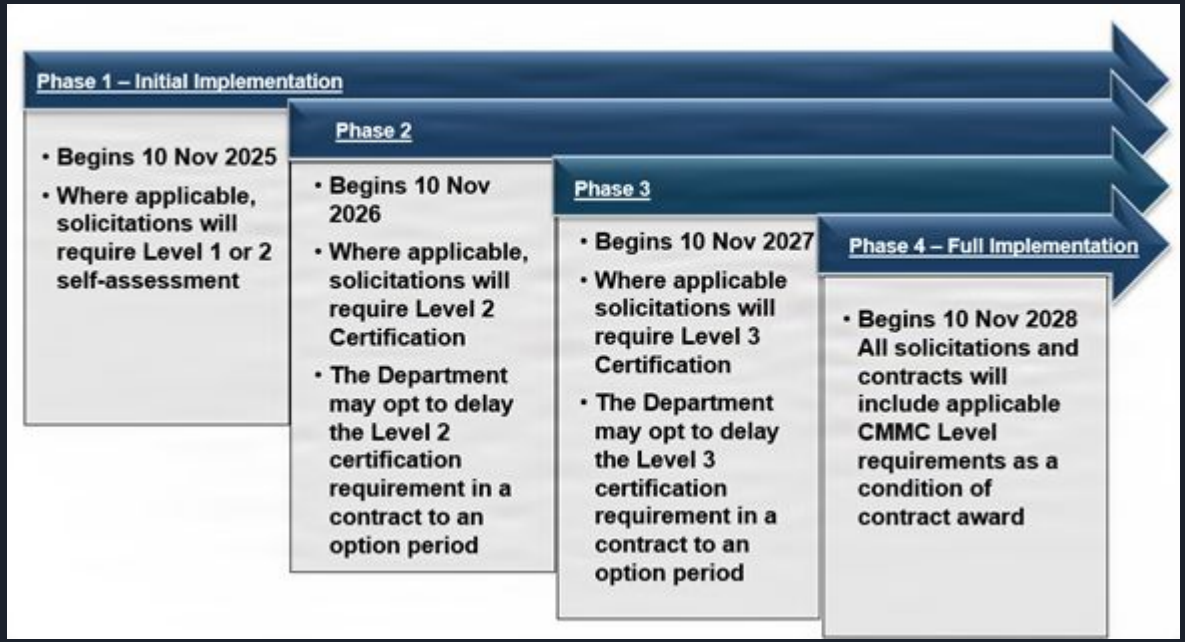
When Does it Start?

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



How Does it Work? CMMC Levels Explained

CMMC Implementation Phase 1

Nov 10th 2025 – Nov 9th 2026

We are currently in phase 1 of CMMC implementation, which means:

Self-Assessment

Level 1 and 2 are both self-assessment during this period

New Contracts

CMMC can be included in any new contract

No C3PAO Required

No third party auditor is required to complete this process

Action Required

If you haven't started, you aren't in violation yet, but risk losing contracts soon!

Roadmap to Compliance

1. Identify Key Team Members
Identify internal and external participants in the process

2. Scope the Environment
Define the people, systems, and processes that handle FCI/CUI

3. Initial Self-Assessment
Start with a basic assessment to find and understand gaps

4. Compile Evidence
Document CMMC-related policies, procedures, and configurations

5. Remediate Gaps
Correct issues using internal or external support as needed

6. Submit Score in SPRS
Enter final score and affirmation after meeting all requirements

Who Is Involved in CMMC Compliance?

Senior Leadership

Must be involved for visibility; they will be signing off on final affirmation!

Internal IT Staff

Any internal staff members who are responsible for the organization's IT

External IT Providers

Any external IT providers should be involved as early as possible in the process

FCI/CUI Employees

Employees who handle FCI/CUI must be aware of specific CMMC requirements

All Employees

All employees should be aware of what FCI/CUI is and the importance of protecting it

Assessment Scoping

Requirement: Prior to conducting a Level 1 self-assessment, the Organization Seeking Assessment (OSA) must specify the CMMC Assessment Scope

- **Level 1:** Assets processing, storing, or transmitting FCI are in scope
- **Level 3:** Assets processing, storing, or transmitting CUI are in scope

Why Scoping is Critical

Risk: Over-Scoping

Too big of a scope creates more work and time

Risk: Under-Scoping

Too small of a scope may mean missing devices and data that should be in scope

Managed Services

Don't forget MSPs; if they store or access your data, they are in scope

Cloud Data

Cloud environments storing CUI/FCI must meet minimum security requirements

How to Minimize Scope

1. Map the Flow
Identify where you handle FCI/CUI today and create a map to track this flow

2. Eliminate Excess
Identify unnecessary devices and users to be eliminated from the data flow

3. Isolate Systems
Isolate systems handling FCI/CUI physically or logically from the network

4. Limit Access
Restrict access to only those authorized and part of the CMMC environment

5. Document Everything
Document as you go, starting from the current state through all changes

Data Flow Mapping Tips

1. Trace & Identify

Track the flow of FCI/CUI across your environment and identify everyone and everything that touches it today

2. Minimize Access

Evaluate if all users and devices truly require access. Strategically reduce the number of touchpoints that process, store, or transmit data

3. Map & Document

Create a final, detailed data flow map that clearly specifies exactly where FCI/CUI is stored, processed, and transmitted

What is a CMMC Enclave?

Isolated Environment

A dedicated, secure environment that separates and protects FCI/CUI devices, data, and users from normal business operations

Automatic Scoping

Everything inside the enclave boundary is automatically in scope, eliminating tough scoping decisions and simplifying compliance

Typical Enclave Components

Workstations *(Data in Use)*
Dedicated physical workstations or virtual machines

Storage *(Data at Rest)*
Securely encrypted storage devices

Network *(Data in Transit)*
A virtual local area network (VLAN) for communication

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)

Understanding Security Requirements

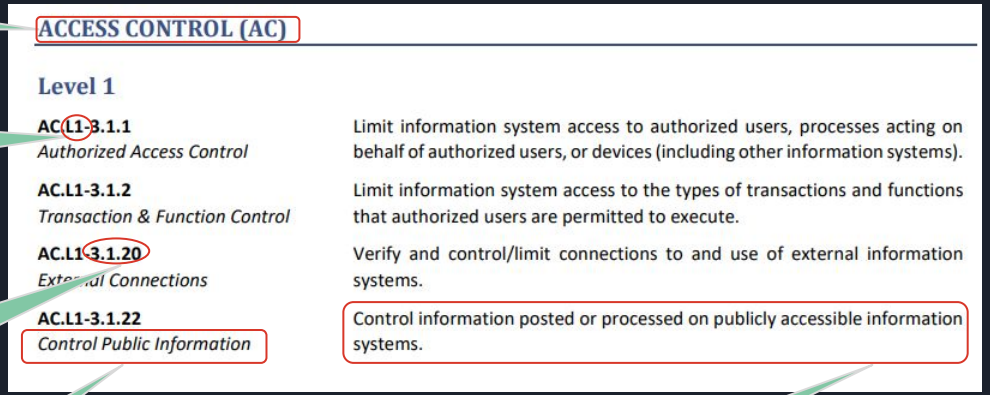
Domain

CMMC Level

Security Requirement #

Short Name Identifier

Complete Practice Statement



ACCESS CONTROL (AC)

Level 1

AC.L1-3.1.1 *Authorized Access Control*	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.L1-3.1.2 *Transaction & Function Control*	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.L1-3.1.20 *External Connections*	Verify and control/limit connections to and use of external information systems.
AC.L1-3.1.22 *Control Public Information*	Control information posted or processed on publicly accessible information systems.

- Each Domain contains individual practices
- Each practice must be satisfied before you can complete a final self or third party assessment
- CMMC Level 1- 17 practices, which include 49 assessment objectives that must be “met”
- CMMC Level 2- 110 practices, which include 320 assessment objectives that must be “met”
- Practices are cumulative!!!!

Access Control (AC) Requirement Example

AC.L1-b.1.i — Authorized Access Control

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

What It Means

Only people who are supposed to have access to your systems and data should have it. Shared accounts, guest accounts left active, and former employees who still have credentials are the most common failures.

What Implementation Looks Like

- **Identity Management:** Active directory or identity management system with individual user accounts
- **Authorized List:** Documented list of authorized users per system
- **Offboarding Process:** Disables accounts on the day of employee departure
- **No Shared Accounts:** No shared or generic accounts (such as "admin" or "IT") used for regular access

Creating Policies

Policy Foundation

If you have no written security policies, you need to create them. All policies should directly reflect the requirements of CMMC

Access Control (AC)

This simple policy covers the Access Control (AC): Controlling system access security requirement (AC.L1-3.1.1)

Example Policy Statement

"Users must log in using their own designated account and are not permitted to share workstations or usernames and passwords. All devices in scope must require unique logins and passwords."

Creating Policies Continued

PE Controls (CMMC Level 1)

This policy covers the four specific physical protection (PE) controls:

- **PE.L1-3.10.1:** Limit physical access to systems, equipment, and environments to authorized individuals
- **PE.L1-3.10.3:** Escort visitors and monitor visitor activity
- **PE.L1-3.10.4:** Maintain audit logs of physical access
- **PE.L1-3.10.5:** Control and manage physical access devices (keys, badges, codes)

Comprehensive Example

"Only Authorized users will be permitted to have physical access to organizational information systems, equipment, and operating environments. Visitors must be escorted and monitored while on premises and a log will be kept to track all physical access by visitors. Only authorized users will be given physical access devices (keys, badges, codes)"

Policy Enforcement

Policy Foundation

Having policies in place is the first step in compliance.

Ensuring those policies are actually in effect is critical.

Auditing & CMMC

Regularly checking that the policies are in place and work in the way they are intended is a CMMC requirement called auditing.

Self-Assessment

Part of the self-assessment process is auditing the policies in your SSP.

Audits should be conducted on a regular basis to ensure successful implementation.

How to Self-Assess

Templates & Guides

Utilize a template! Don’t reinvent the wheel. There are free templates and questionnaires available from reputable sources

CISA Downloadable Tool

CISA offers a downloadable tool that walks you through L1 or L2 self-assessment

Project Spectrum

Offers an online tool to self-assess and track your progress

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

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*

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/