



Southeast Region Federal Construction

2026 SUMMIT

April 14-16 Wilmington, North Carolina

Infrastructure & Environmental Summit

Virginia

North Carolina

South Carolina

Georgia

Florida

Hosted by

US Senator Thom Tillis

US Senator Ted Budd

North Carolina Military Business Center



CMMC READINESS

A Step-By-Step Guide for Contractors

Tim Malone

Regional Program Manager

NC Military Business Center at Cape Fear Community College

THE PROBLEM



Confusion

Multiple levels, changing rules,
conflicting advice from vendors



Paralysis

Contractors delay action, hoping
the requirement goes away



Oversold

Expensive consulting for
problems that don't require it

This session will make CMMC practical, clear, and doable.

DOES CMMC APPLY TO YOU?

The threshold question every contractor should answer first

Federal Contract Information (FCI)

Information provided by or generated for the government under a contract

Not intended for public release

Think: contract details, delivery schedules, project specs not publicly posted


CMMC Level 1

Controlled Unclassified Information (CUI)

Government-created or owned info that requires safeguarding

Marked or should be marked as CUI

Think: technical drawings, vulnerability assessments, personnel data


CMMC Level 2

CMMC LEVEL 1

Protecting Federal Contract Information (FCI)

15

Security
Practices

6

Practice
Domains

Self

Assessment
Type

The Six Domains:

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

Most contractors are already doing many of these. The gap is documentation, not implementation.

CMMC LEVEL 2

Protecting Controlled Unclassified Information (CUI)

110

Security
Controls

14

Control
Families

Self*

Assessment
*During Phase 1

What You Need to Know:

- ✓ Based on NIST SP 800-171 Rev 2 (110 security controls)
- ✓ All 15 Level 1 practices are included in the 110 controls
- ✓ Level 1 work is not wasted. It is the foundation for Level 2
- ✓ Requires a System Security Plan (SSP) and Plan of Action & Milestones (POA&M)

The work you do for Level 1 directly builds toward Level 2 compliance.

YOU ARE IN THE WINDOW

CMMC Phase 1 Implementation

November 10, 2025 — November 9, 2026

Focus: Level 1 and Level 2 self-assessments

What This Means for You:

- ✔ Both Level 1 and Level 2 are self-assessment right now
- ✔ No third-party auditor (C3PAO) required during Phase 1
- ✔ Affirmation must be submitted with your assessment in SPRS
- ✔ Use this time to get your house in order before requirements tighten

SCOPING AS STRATEGY

The single most important decision in your compliance journey

The smaller your scope, the smaller your compliance burden.

The Common Mistake

Treating the entire business as in-scope

Every laptop, every employee, every network segment must meet all controls

Massive effort. Massive cost. Most of it unnecessary.

The Smart Approach

Define a tight boundary around where FCI/CUI actually lives

Only the systems, people, and processes that touch sensitive data are in scope

Focused effort. Manageable cost. Achievable timeline.

MINIMIZING YOUR SCOPE

Ask yourself: Where does sensitive data actually live and move?



Identify

Where do you receive, store, and transmit FCI or CUI? Map the actual data flow.



Isolate

Separate the systems that handle sensitive data from your general business network.



Limit Access

Only the people who need to touch FCI/CUI should have access to the scoped environment.



Document

Clearly define your scope boundary in writing. This becomes part of your assessment evidence.





A well-defined scope turns a company-wide project into a manageable, focused task.

THE ENCLAVE CONCEPT

A dedicated, isolated environment where sensitive data lives

YOUR GENERAL BUSINESS NETWORK

CUI ENCLAVE

-  Dedicated workstation(s)
-  Segmented network (VLAN)
-  Controlled access / MFA
-  Encrypted storage

Outside the enclave:

- Email (personal)
- General office PCs
- Accounting systems
- Personal devices

Everything outside the enclave boundary is out of scope for CMMC assessment.



BUILDING A VIRTUAL ENCLAVE

You don't need a separate physical office. You need a logical boundary.

Dedicated Machine or VM

A single laptop, desktop, or virtual machine used only for CUI work. Not shared with general business tasks.

Separate Network Segment

A VLAN or separate Wi-Fi network that isolates the enclave from your general business traffic.

Controlled User Access

Only authorized personnel log in. Multi-factor authentication enforced. Access logged.

Encrypted Storage

Full disk encryption on the device. CUI at rest is protected even if hardware is lost or stolen.

Defined Data Flow

Clear rules for how CUI enters and exits the enclave. No emailing CUI from personal accounts.

For many construction contractors, this could be as simple as one laptop on a separate VLAN.

THE COMPLIANCE PROCESS

Four steps from start to submission

1

Scope Your Environment

Define what systems, people, and processes handle FCI/CUI

2

Assess Against Controls

Evaluate your current state against the required practices

3

Build Your Evidence Pack

Document policies, configurations, and proof of compliance

4

Submit Score in SPRS

Enter your score and complete the executive affirmation

This process applies to both Level 1 and Level 2. The difference during Phase 1: both are self-assessed.

RESOURCES

Everything you need to get started is free and publicly available



DoD CIO CMMC Page

dodcio.defense.gov/cmmc

Official guides, scoping documentation, assessment resources, and the latest implementation timeline

NIST SP 800-171 Rev 2

The 110 security controls that define Level 2 requirements

Supplier Performance Risk System (SPRS)

Where you submit your assessment score and affirmation

CMMC Scoping Guides

Available on the DoD CIO page for both Level 1 and Level 2

Cyber AB Marketplace

Find Registered Practitioners and C3PAOs when needed



QUESTIONS?

Tim Malone

Regional Program Manager
NC Military Business Center
at Cape Fear Community College

dodcio.defense.gov/cmmc