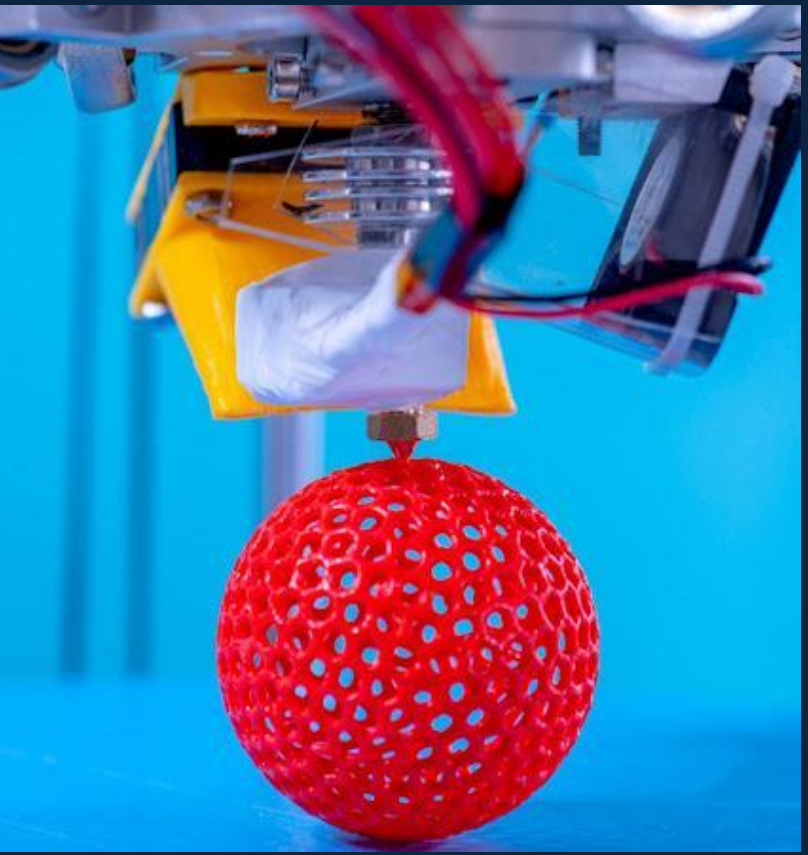


Who is Industry Extension Services?

University Extension Partner with business and industry to transfer knowledge and support next-generation technologies.

A Public/Private Performance Model:

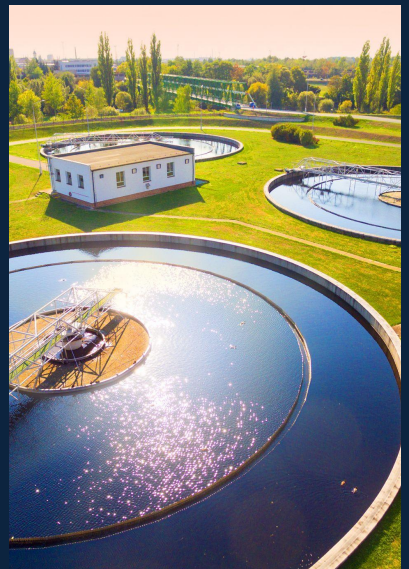
- State Appropriations
- Federal Funding
- Revenue-based Activities

Industries Served:

- Small-medium Size Manufacturers
- Educational and Research Institutions
- Healthcare and Pharmaceutical Companies
- Defense Contractors
- Aerospace and Energy Sectors
- Government Agencies

ies.ncsu.edu

We Can Help.



Expertise

- Advanced Manufacturing + Technology Adoption
- Business Growth, Innovation + Marketing Solutions
- Cybersecurity Strategies
- Defense Industry Initiatives
- Energy + Environmental Solutions
- Grant Evaluation + Research
- Instructional Design Services
- Leadership + Organizational Coaching
- Process Optimization + Training Within Industry
- Quality + Management Systems
- Supply Chain Optimization + Supplier Matching
- Workplace Health + Safety

ies.ncsu.edu

We Can Help.

CMMC Level 1- Part 3, Implementation & Documentation

NC STATE UNIVERSITY

Industry Extension Services

IES Presents: Streamlining CMMC Compliance Series, Part 3

Unexpected News...

RELEASE

IMMEDIATE RELEASE

Forging the Arsenal of Freedom: Department of War Suspends CMMC Phase II Requirements

July 13, 2026 |

The Department of War today announces the immediate suspension of the Cybersecurity Maturity Model Certification (CMMC) Phase II requirements, which were originally scheduled to come into effect on November 10, 2026. All Phase I self-assessment requirements remain firmly in place. Additionally, the Department will begin a comprehensive review of CMMC aimed at aligning with Secretary of War Pete Hegseth's Acquisition Transformation System (ATS) directives prioritizing speed to capability, lowering barriers for small, medium, and non-traditional businesses, and replacing bureaucratic compliance with scalable, resilient cybersecurity measures.

> *In support of Secretary Pete Hegseth's directive to reduce compliance barriers for small and medium sized businesses, we are today suspending the CMMC Phase II requirements and initiating a 60-day study of the future of this program...*
>
> **— Department of War Release, 7/13/26**

What We Know About CMMC Today

CMMC Reform Task Force

Currently conducting a top-to-bottom 60-day review of the certification program.

"The mandate of this Task Force is to provide recommendations for a reformed framework that prioritizes speed to capability, lowers barriers... and replaces prohibitive, third-party compliance models with scalable, realistic security measures".

Baseline Compliance Enforced

During suspension, DoD will continue enforcing baseline compliance with NIST SP 800-171 Rev 2 via DIB self assessments

DFARS Clause Still Active

Cybersecurity requirements outlined in DFARS clause 252.204-7012 (Safeguarding & Incident Reporting) remain in effect

DoW Soliciting RFI Input

Contractor input is due by August 14th via RFI to help understand the burdens and constraints of the CMMC program

Some Assumptions Based on DoW Language

CMMC Program is Not Going Away

Nothing in the public announcement signaled the program would be retired. It will likely be a more streamlined version of the current CMMC program

Third-Party Requirements

The CMMC program will likely remove third-party requirements

New Implementation Timeline

All current program milestones (November 2026, 2027, 2028) will likely be replaced with a new timeline for implementation and phased roll out

Continued Cyber Controls

There will be a continued effort to require DoD contractors to implement cyber controls and report their current status to the DoD

The "60-Day" Review Reality

The DoD announced it would launch a 60-day review in 2021… which transitioned into a 6-month review, and eventually turned into nearly 3 years of rulemaking.

This is not likely to be resolved in 60 days

Fair Warning!

DFARS 252.204-7020

Allows the department to show up with DIBCAC and evaluate your cybersecurity posture. Unchanged since 2020.

⚠️ ***Audit Risk:*** *Working with the DoD means they can audit your cybersecurity at any time!*

DFARS 252.204-7021

Requires contractors to maintain current CMMC status for the duration of the contract and submit annual affirmations.

⚠️ ***Continuous Compliance:*** *Must be maintained throughout the contract, not just before affirmations.*

False Claims Act (FCA)

In effect to investigate and prosecute contractors who knowingly misrepresent their cybersecurity compliance.

⚠️ ***Prosecution Risk:*** *FCA claims are active; do not let your guard down due to program pauses or delays.*

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)

Information provided by or created for the government as part of a contract

Not intended for public release

Examples: *Contract details, building specs not on SAM, project schedules, and CO communications*

✅ CMMC LEVEL 2

Controlled Unclassified Information

Government-created or owned info that requires safeguarding

(SHOULD) Be marked CUI

Examples: *Engineering drawings, SSNs, financial data, trade secrets, and applicant data*

Ask the prime or contracting officer to clarify if you can't find FAR or DFARS clause in current contract!!

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

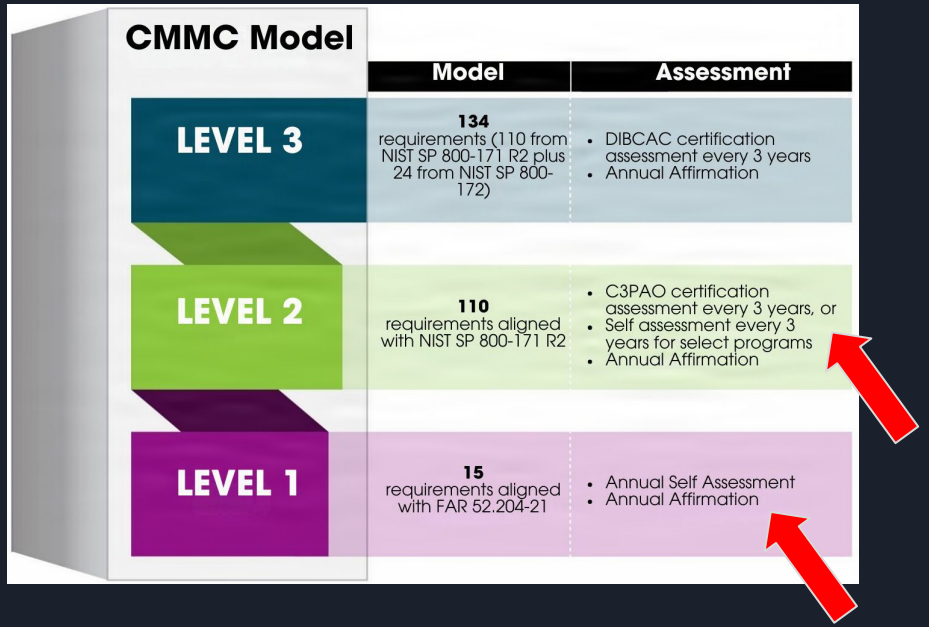
Fourteen Security Domains (AKA Control Families)

- 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



Section 3: Finishing the Job- CMMC Compliance

CUI Tips & Tricks

1. Contractor Responsibility

Ask the prime contractor to mark all FCI and CUI, it is their responsibility to ensure all data is properly designated.

2. Unlabeled Data Protocol

If shared data is unlabeled, request confirmation immediately. Assume it is not CUI, but prompt them to clarify so you can take appropriate action.

3. Internal Markings

Mark all FCI/CUI internally. Ensuring proper label visibility helps all employees understand the mandatory steps required to protect it.

4. System Verification

Quickly identify if CUI reaches an unauthorized system. If CUI is sent to an unequipped system, immediately alert the disseminating agency.

Scoping Tips

People

- Consultants who provide cybersecurity service
- Managed service provider personnel who implement system maintenance
- Enterprise network administrators

Technology

- Cloud-based security solutions
- Hosted Virtual Private Network (VPN) services
- SIEM solutions

Facilities

- Co-located data centers
- Security Operations Centers (SOCs)
- OSA office buildings

- People, devices, and facilities are in scope if they handle FCI (L1) or CUI (L2)
- Major changes require scoping/assessment update*

Scoping Tips: CMMC Level 1

Level 1 Scope: FCI Assets

All assets that process, store, or transmit Federal Contract Information (FCI).

- **Process:** FCI is accessed, entered, edited, or manipulated
- **Store:** FCI is inactive on electronic media or physical documents
- **Transmit:** FCI is being transferred between assets

Specialized Assets

Assets that handle FCI but cannot be fully secured (e.g., IoT, IIoT, OT). Document, but exclude from CMMC assessment

Out of Scope

Specialized Assets are not part of the Level 1 self-assessment scope and are not assessed against CMMC requirements

Scoping Tips: CMMC Level 2

CUI Asset Scope

Assets that process, store, or transmit Controlled Unclassified Information (CUI).

- **Process:** CUI is used, accessed, or edited by an asset
- **Store:** CUI is at rest on media, memory, or physical format
- **Transmit:** CUI is transferred between assets

OSA Requirements

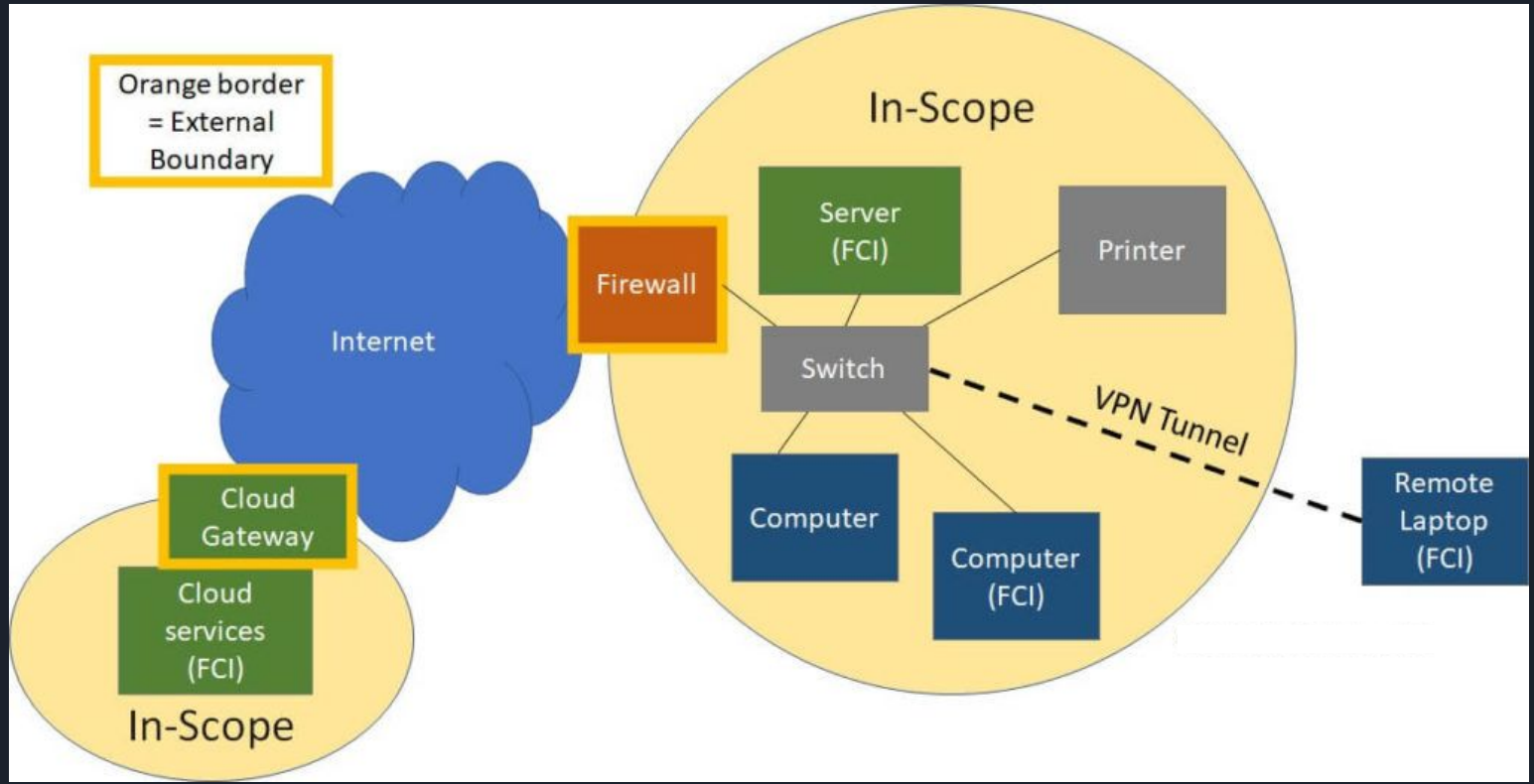
- Inventory all assets (embedding in SSP not required)
- Document asset treatment in the SSP
- Provide network diagrams to facilitate scoping

Specialized Assets

In scope and protected by existing policies, but not assessed against CMMC requirements

DOCUMENT THEM!

Scoping: Network Diagram Example



Conduct Self-Assessment

Assessment Methods

Use a printed questionnaire, digital template, or automated tool to record current status

Status: "Met"

Provide concise notes explaining how the control requirements are being satisfied

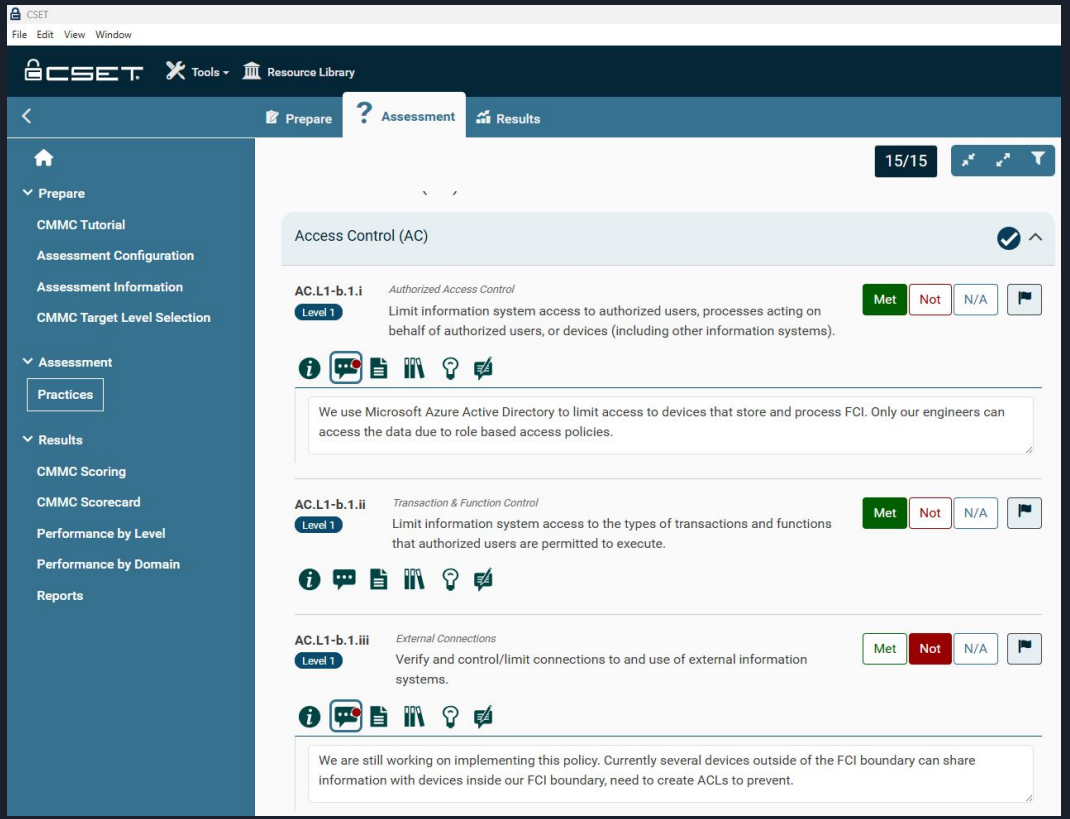
Status: "Not Met"

Detail what is missing and document any existing policies or procedures currently in place

CMMC controls are binary ("met" or "not met"). Perform as many assessments as needed

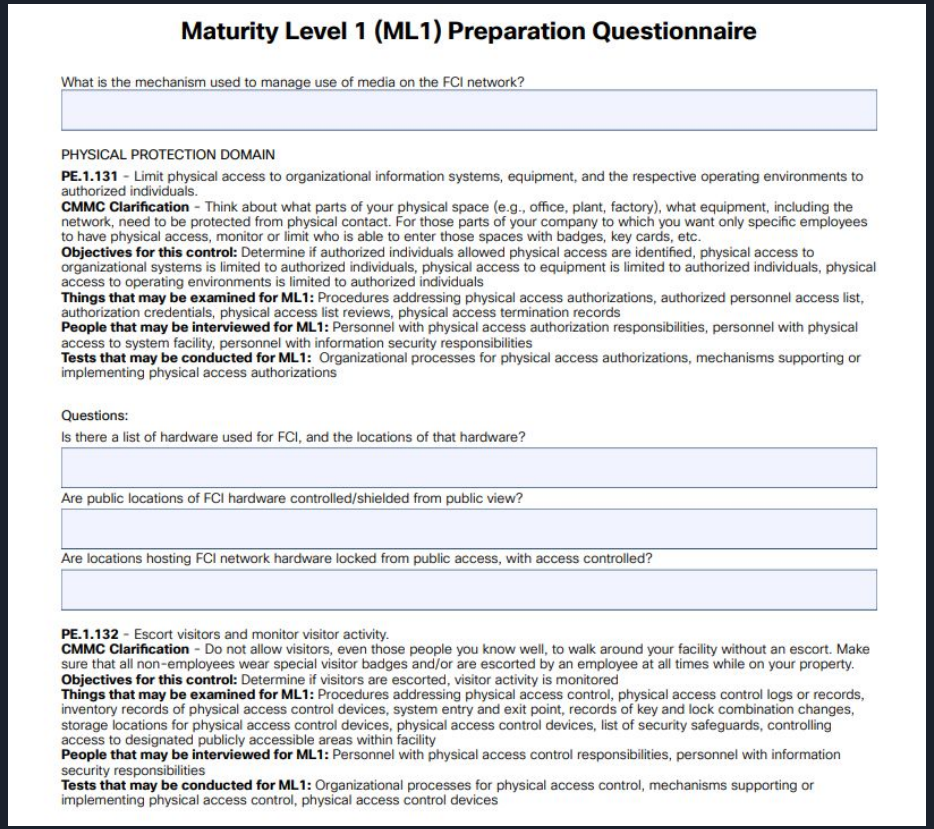
Digital Self-Assessment Tools

- Tools like this one are easy to understand and guide you through the process
- The tool helps explain CMMC requirements as you go through
- At the end, you get a report that can be saved, exported, or updated in the future



Self-Assessment Using Questionnaire

- If you prefer to work offline, downloadable templates/questionnaires are readily available
- You can print or utilize a downloadable template
- The downside is lack of automation, reports, and the ability to edit



Maturity Level 1 (ML1) Preparation Questionnaire

What is the mechanism used to manage use of media on the FCI network?

PHYSICAL PROTECTION DOMAIN

PE.1.131 - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
CMMC Clarification - Think about what parts of your physical space (e.g., office, plant, factory), what equipment, including the network, need to be protected from physical contact. For those parts of your company to which you want only specific employees to have physical access, monitor or limit who is able to enter those spaces with badges, key cards, etc.
Objectives for this control: Determine if authorized individuals allowed physical access are identified, physical access to organizational systems is limited to authorized individuals, physical access to equipment is limited to authorized individuals, physical access to operating environments is limited to authorized individuals
Things that may be examined for ML1: Procedures addressing physical access authorizations, authorized personnel access list, authorization credentials, physical access list reviews, physical access termination records
People that may be interviewed for ML1: Personnel with physical access authorization responsibilities, personnel with physical access to system facility, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for physical access authorizations, mechanisms supporting or implementing physical access authorizations

Questions:

Is there a list of hardware used for FCI, and the locations of that hardware?

Are public locations of FCI hardware controlled/shielded from public view?

Are locations hosting FCI network hardware locked from public access, with access controlled?

PE.1.132 - Escort visitors and monitor visitor activity.
CMMC Clarification - Do not allow visitors, even those people you know well, to walk around your facility without an escort. Make sure that all non-employees wear special visitor badges and/or are escorted by an employee at all times while on your property.
Objectives for this control: Determine if visitors are escorted, visitor activity is monitored
Things that may be examined for ML1: Procedures addressing physical access control, physical access control logs or records, inventory records of physical access control devices, system entry and exit point, records of key and lock combination changes, storage locations for physical access control devices, physical access control devices, list of security safeguards, controlling access to designated publicly accessible areas within facility
People that may be interviewed for ML1: Personnel with physical access control responsibilities, personnel with information security responsibilities
Tests that may be conducted for ML1: Organizational processes for physical access control, mechanisms supporting or implementing physical access control, physical access control devices

Where do Submit Compliance Information?

- The Supplier Performance Risk System (SPRS) is the location for vendors to certify CMMC Level 1 and Level 2 compliance and for the defense acquisition community to review
- SPRS is where initial assessments and annual affirmation will be conducted
- Vendors must be registered in the System for Award Management (SAM) before registering in Procurement Integrated Enterprise Environment (PIEE)

SPRS has step by step video training to guide you through the process!!

What Do I Upload in SPRS to be Compliant?

- First a New CMMC Assessment must be added in your SPRS account
- Next enter assessment data, selecting “Met”, “Not Met”, or “N/A” for each requirement
- Review all answers are accurate and complete
- Assessment scope, employee count, and CAGE code are required
- Finally, submit for Affirmation

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/

NC STATE UNIVERSITY Industry Extension Services

Chris McGraw
Western
828.329.3119
chris_mcgraw@ncsu.edu

Kami Baggett
Piedmont Triad
919.830.7292
kameron_baggett@ncsu.edu

Mary Tillery
Central
910.622.5849
mary_tillery@ncsu.edu

Mitch Poteat
Research Triangle
919.607.0684
mitch_poteat@ncsu.edu

Robert Crew
Wake County
919.830.2941
robert_crew@ncsu.edu

Lori Benn
Northeast
919.988.7475
lori_benn@ncsu.edu

Jennifer Fielder
Charlotte Proper
704.728.7554
jennifer_fielder@ncsu.edu

Tamara Mack
Greater Charlotte
980.281.0939
tamara_mack@ncsu.edu

Anna Mangum
South Central
919.210.6050
anna_mangum@ncsu.edu

Regional Managers

ncstateies.com/RM

We Can Help.

Thank You!