

Southeast Region Federal Construction

2025 SUMMIT

April 22-24 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

Southeast Region Federal Construction

2025 SUMMIT

April 22-24 Wilmington, North Carolina

Infrastructure & Environmental Summit

Virginia

North Carolina

South Carolina

Georgia

Florida

THANK YOU PROGRAM SPONSORS

Black & Veatch

CCI Prime Contractors LLC

CMMC Certification for Infrastructure Contractors

Southeast Region Federal Construction

2025 SUMMIT

April 22-24 Wilmington, North Carolina

Infrastructure & Environmental Summit

Virginia North Carolina South Carolina Georgia Florida

Laura Rodgers, Director of Cybersecurity Practice, Secure Computing Institute and Director,
NC-PaCE, NC State University

CMMC For Infrastructure Contractors

2025 SE Region Federal Construction/Infrastructure/Environmental Summit

April 24, 2025

About Me



LOCKHEED MARTIN MISSILE
PROGRAMS



GENERAL DYNAMICS IT –
SOLDIER TRAINING PROGRAMS



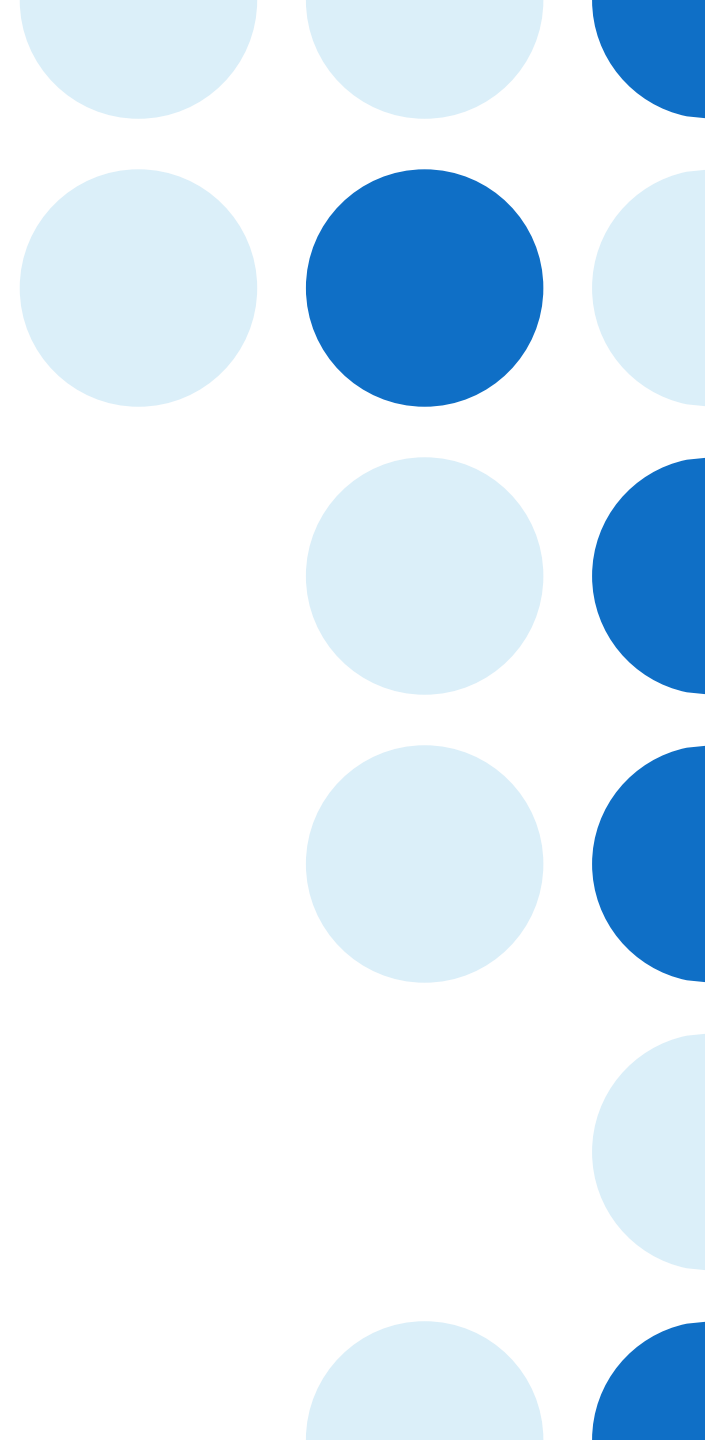
30 YEARS EXPERIENCE IN GRC
AND POLICY



BEGAN TEACHING
CYBERSECURITY COMPLIANCE
FOR DEFENSE CONTRACTORS IN
2020

Agenda

- Two CMMC rules
 - CMMC program Model
 - CMMC levels
 - CMMC timeline
 - Cyber threats - unique to infrastructure contractors
 - What you should be doing now to prepare
 - Resources
-



Waivers of CMMC Requirement

Waivers are done at the contract level, not the contractor level.

Goal – Big Picture

To keep our country's sensitive data out of the hands of our adversaries.

When you get stuck in the weeds, take a step back and remember the intent (goal) of the regulation and the standard.

You want the right people having access to the right information at the right time.

Why CMMC?

Our adversaries
continue to steal
our technology.

Self-assessments
provide a low level
of confidence that
contractors'
systems are secure.

Not enough DoD
assessors
(DIBCAC)

CMMC – All About Protecting Data



Federal contract information (FCI) - information that is created or provided by the U.S. federal government as part of a contract but is not intended for public release.



Controlled unclassified information (CUI) - information that is created or provided by the U.S. federal government as part of a contract that is unclassified but still requires safeguarding and dissemination controls.

<https://www.archives.gov/cui/registry/category-list>

NOTE: CMMC does not apply to *strictly* COTS

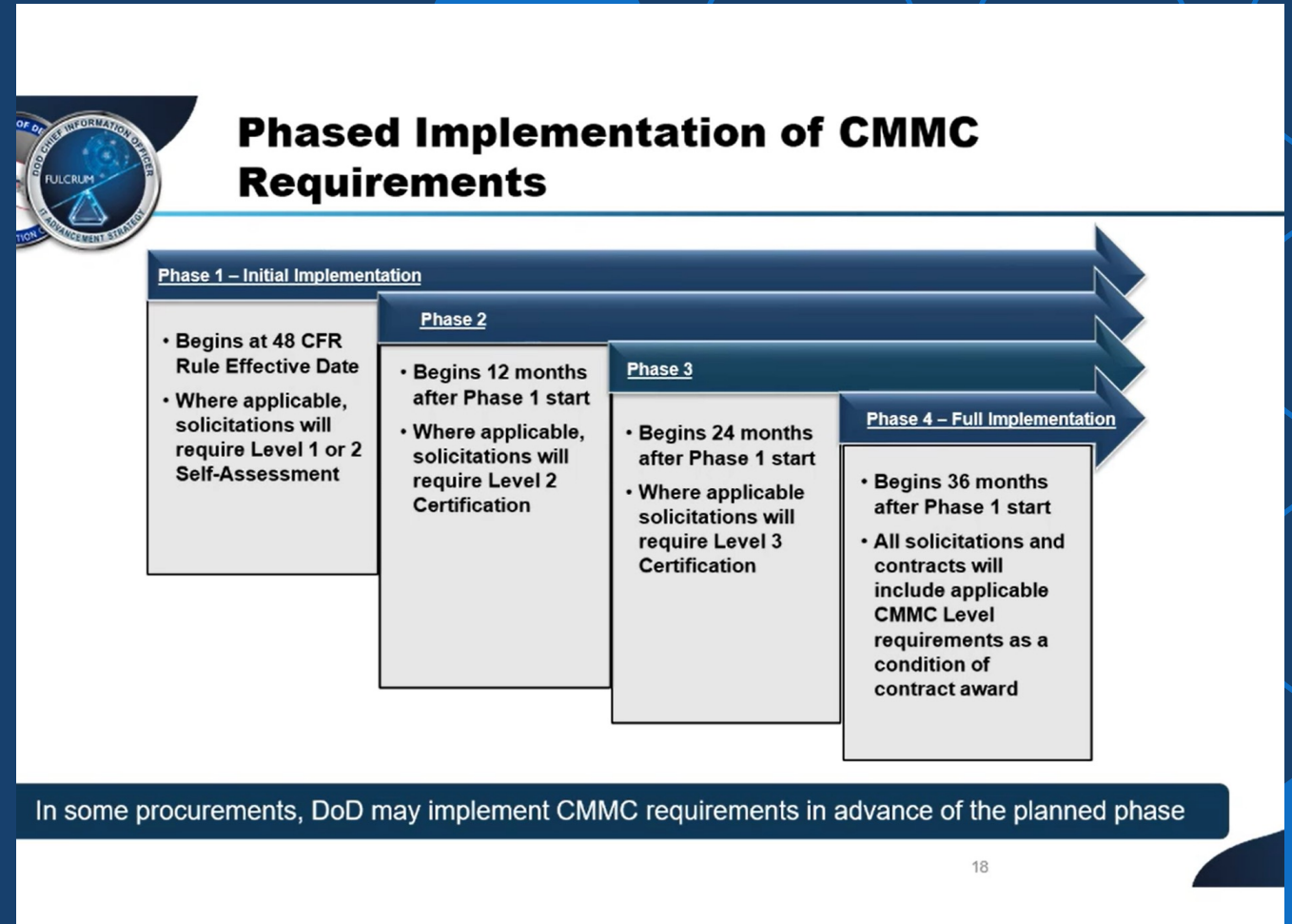
CMMC Rules

The 32 CFR Part 170 rule established CMMC as a ***program***. *Effective 12.16.24.*

The 48 CFR Part 204 rule provides information about *including CMMC in contracts*, including DFARS 252.204-7021, the CMMC clause. Effective date: summer 2025. Rolled out over several years, through 2028.

CMMC Estimated Timeline

Inclusion of CMMC Program Requirements in solicitations and contracts will occur over four phases and will roll out incrementally until 2028.



CMMC is an **assessment model**
– the security controls for most
of the DIB did not change.

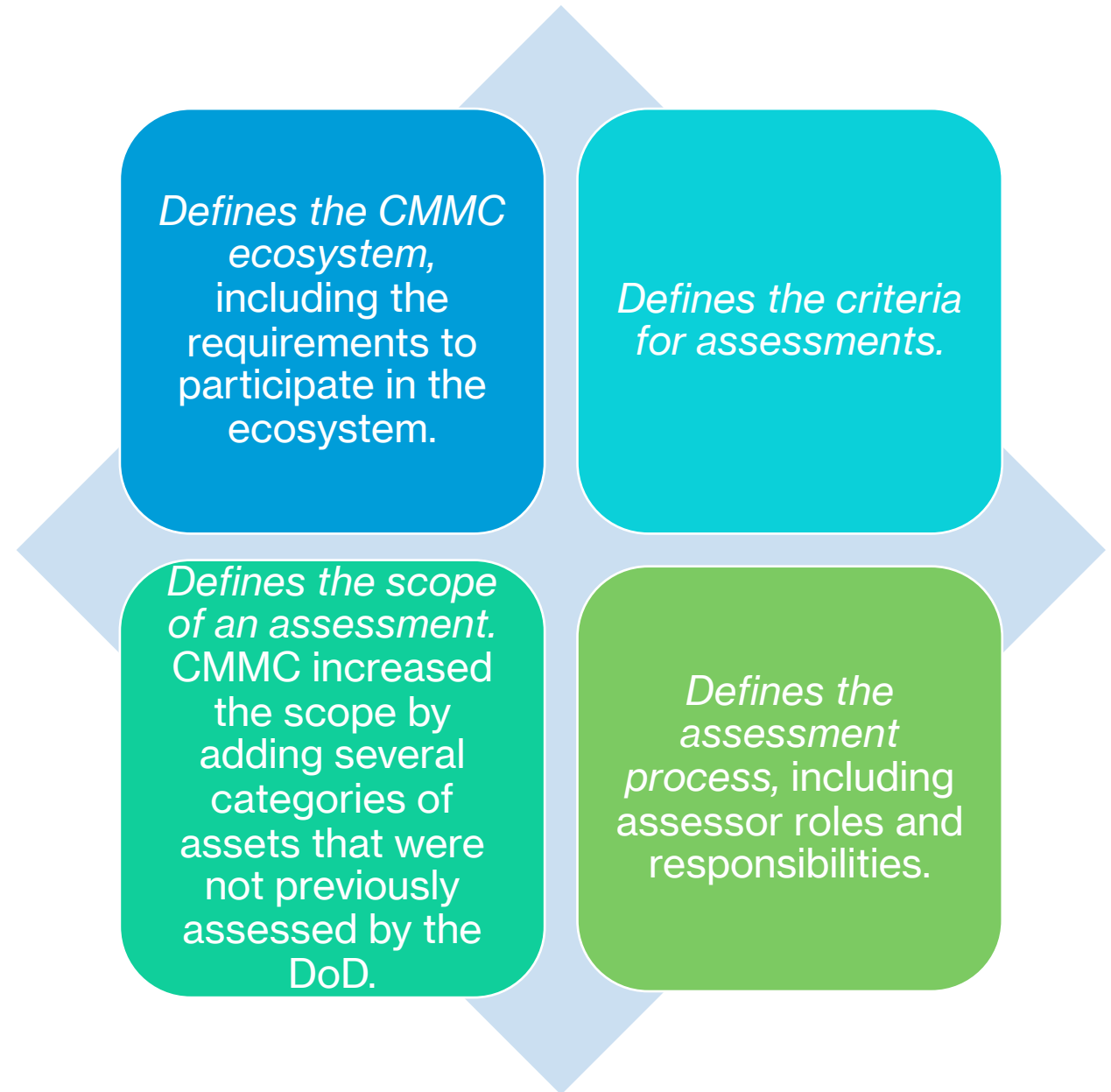
Level 3 = CUI + APT/HVA

Level 2 = DFARS 252.204-7012,
paragraph (b)(2)(i) - (Protection
of Controlled Unclassified
Information - CUI)

Level 1 = FAR 52.204-21
(Protection of Federal Contract
Information - FCI)

CMMC Model		
	Model	Assessment
LEVEL 3	134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171 r2	• C3PAO assessment every 3 years, or • Self-assessment every 3 years for select programs. • Annual Affirmation
LEVEL 1	15 requirements aligned with FAR 52.204-21	• Annual self-assessment • Annual Affirmation

CMMC Program Rule



CMMC Level 1

Implement 15 basic security controls to protect Federal Contract Information (FCI).

Scope – any asset that processes, stores, and/or transmits FCI. Includes external service providers that handle FCI.

Pass/Fail – NO SCORE; all controls must be implemented fully to claim CMMC Level 1 compliance.

No Plan of Action and Milestones (POAM) permitted

Annual self-assessment

Annual affirmation of compliance by a senior-level company representative

Very few contractors will be allowed to assess at CMMC Level 1

CMMC Level 1 = FAR 52.204-21

Basic Safeguarding of Covered Contractor Information Systems

CMMC Level 1 = 15 basic security controls in FAR 52.204-21

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

CMMC Level 2

- Implement the 320 assessment objectives in the 110 security controls in NIST SP 800-171 r2 to protect CUI
 - Some self-assessments; mostly 3rd party assessment – every 3 years, annual affirmation
 - Very limited use of POAMs – must be closed out in 180 days
 - Scope
 - CUI Assets – assets that process, store, and/or transmit CUI
 - Security Protection Assets – assets that provide security functions to in-scope assets. May not be fully assessed but must be documented in the asset inventory SSP, and network diagram.
 - Specialized Assets – assets such as IoT, OT GFE that are unable to be fully secured. Must be documented in the asset inventory, SSP, and network diagram.
 - Contractor Risk Managed Assets – assets that can, but are not intended to, process, store, or transmit CUI.
-

CMMC Level 3

Full implementation of NIST SP 800-171 r2 plus 24 controls in NIST SP 800-172 to protect high-risk CUI

Third party assessment for Level 2, DIBCAC assessment for 24 controls in NIST SP 800-172

Very limited use of POAMs – must be closed out in 180 days

Scope similar to Level 2

PPT = People- Process-Technology Framework

PEOPLE – PROCESS – TECHNOLOGY

In cybersecurity, people are more important than processes or technology.



Unique Cyber Threats - Infrastructure Contractors

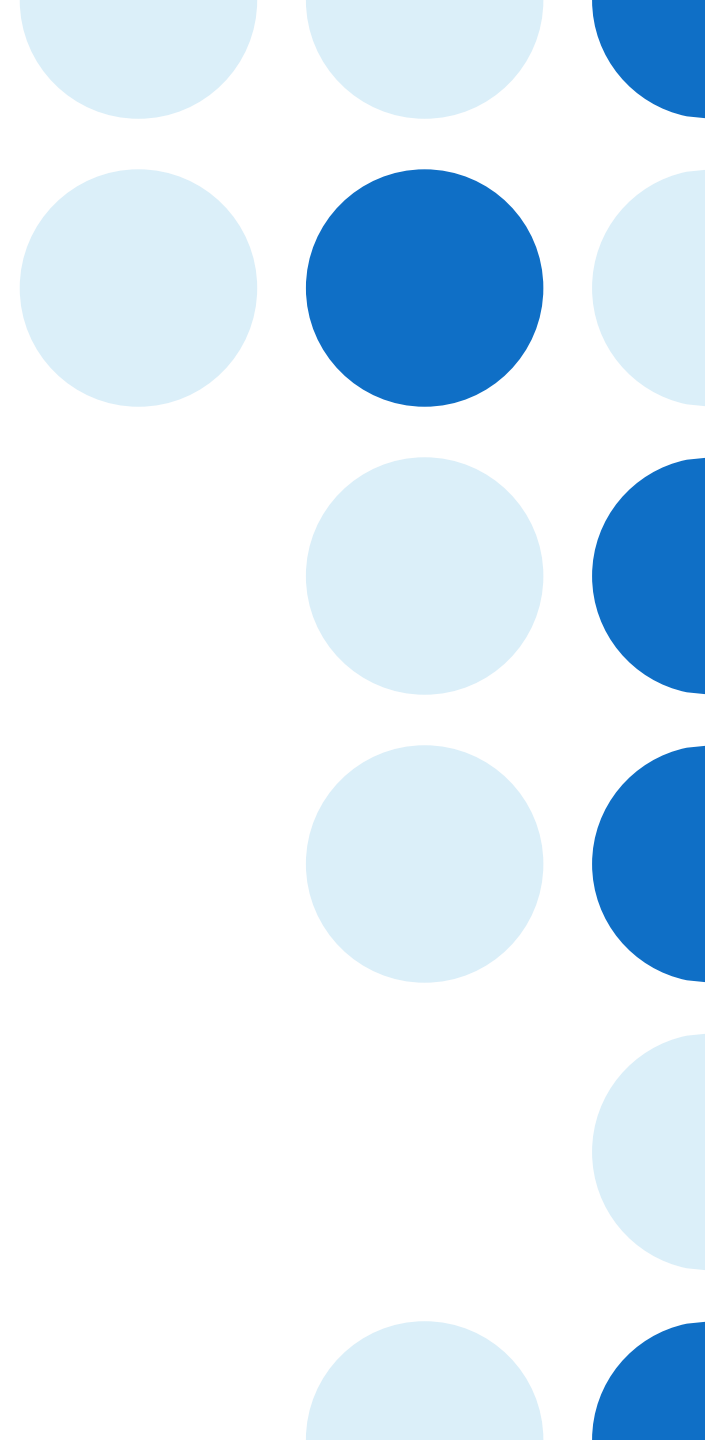
Supply chain attacks - lots of subs/suppliers in construction supply chains

Use of digital tools, such as building info. modeling, and IoT devices increases attack surface

Confusion about CUI

Supply Chain Risk Mitigation

- Conduct thorough risk assessments of your supply chain
 - ✓ Identify and prioritize critical assets in your supply chain that are most vulnerable to cyber attacks
 - Reduce choke points - have multiple vendors for critical items/services (if possible)
 - Create contingency plans to manage potential supply chain disruptions
 - Communicate with subs/suppliers
 - ✓ Encourage the use of free NSA and DC3-DCISE cybersecurity tools and services (links in resources section)
 - ✓ Provide links to training
 - Include cyber requirements in contracts only if necessary (sub/supplier handles FCI/CUI)
 - Limit vendor access and privileges - provide access to only what they need to perform the work
-



Supply Chain Risk Mitigation

- Assess the cybersecurity posture of organizations in your supply chain. Typically done using questionnaires:
 - ✓ For subs/suppliers that only handle **FCI**, use the 15 requirements in FAR 52.204-21 to develop the questionnaire
 - ✓ Questionnaire for subs/suppliers that handle **CUI**, use the 15 requirements in the FAR clause, plus the following:
 - ✓ Does the company provide ongoing cybersecurity training for its employees?
 - ✓ Does the company implement MFA on all accounts?
 - ✓ Does the company update/patch systems regularly?
 - ✓ Does the company implement encrypt sensitive data in transit and at rest?
 - ✓ Does the company have a written incident response plan?
-

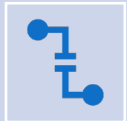
Securing IoT devices



Change default passwords on devices

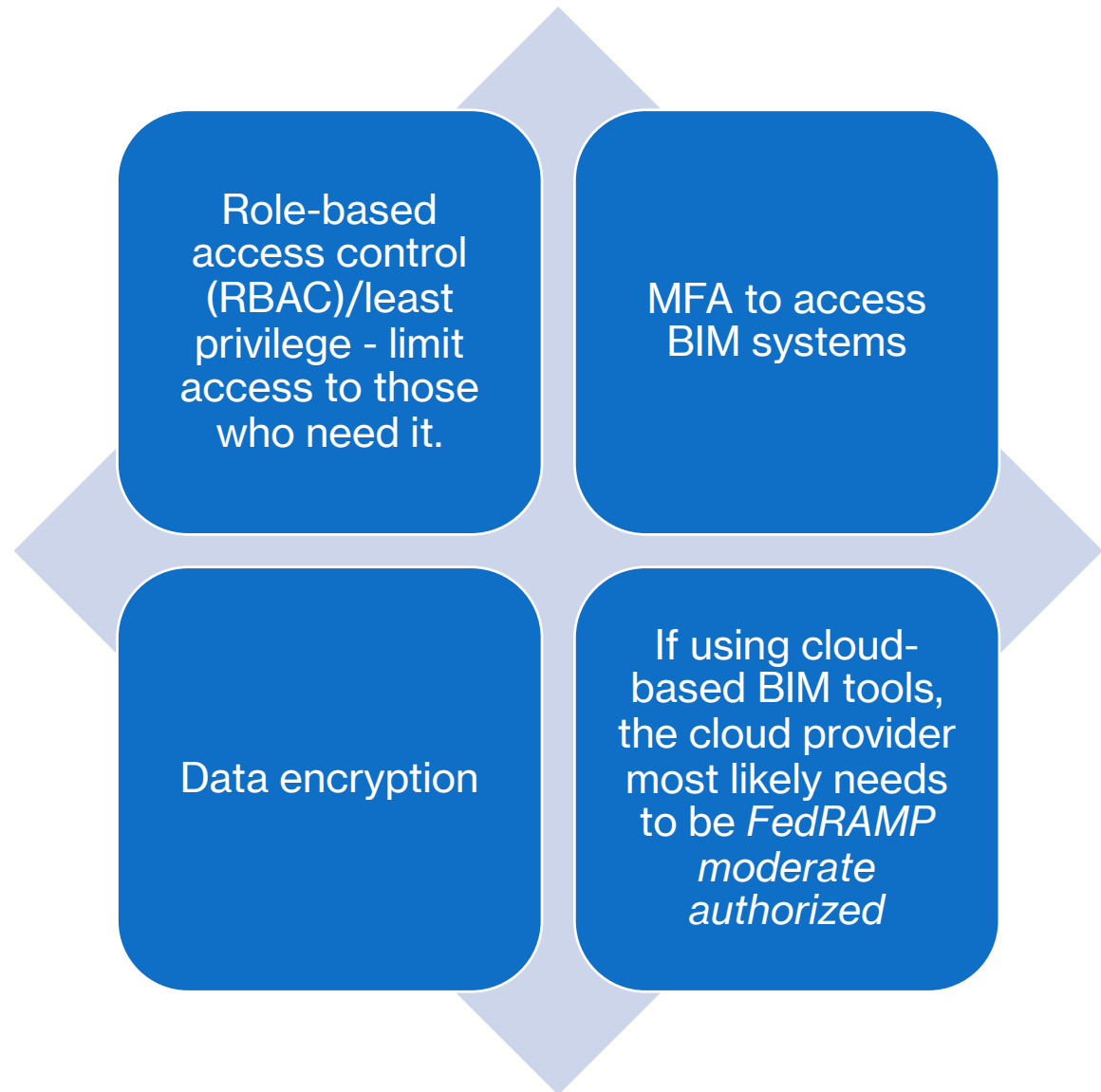


If device supports MFA, use it



Put IoT devices on a separate network segment from your other systems - firewalls between segments, VLANs, switches/routers, VPNs.

Securing Digital Tools



CUI Confusion

- CUI in construction
 - Specs/standards
 - Engineering drawings
 - Process sheets
 - Manuals
 - Technical reports
 - Technical orders
 - Data sets
 - Studies/analyses
 - Software executable code
 - Source code

- Source: National Archives CUI Registry:

<https://www.archives.gov/cui/registry/category-list>

Remember: CUI data that belongs to the DoD determines the scope of your assessment.

Other sensitive information, such as employee PII, should be protected at the same level as DoD CUI, but not comingled with it.

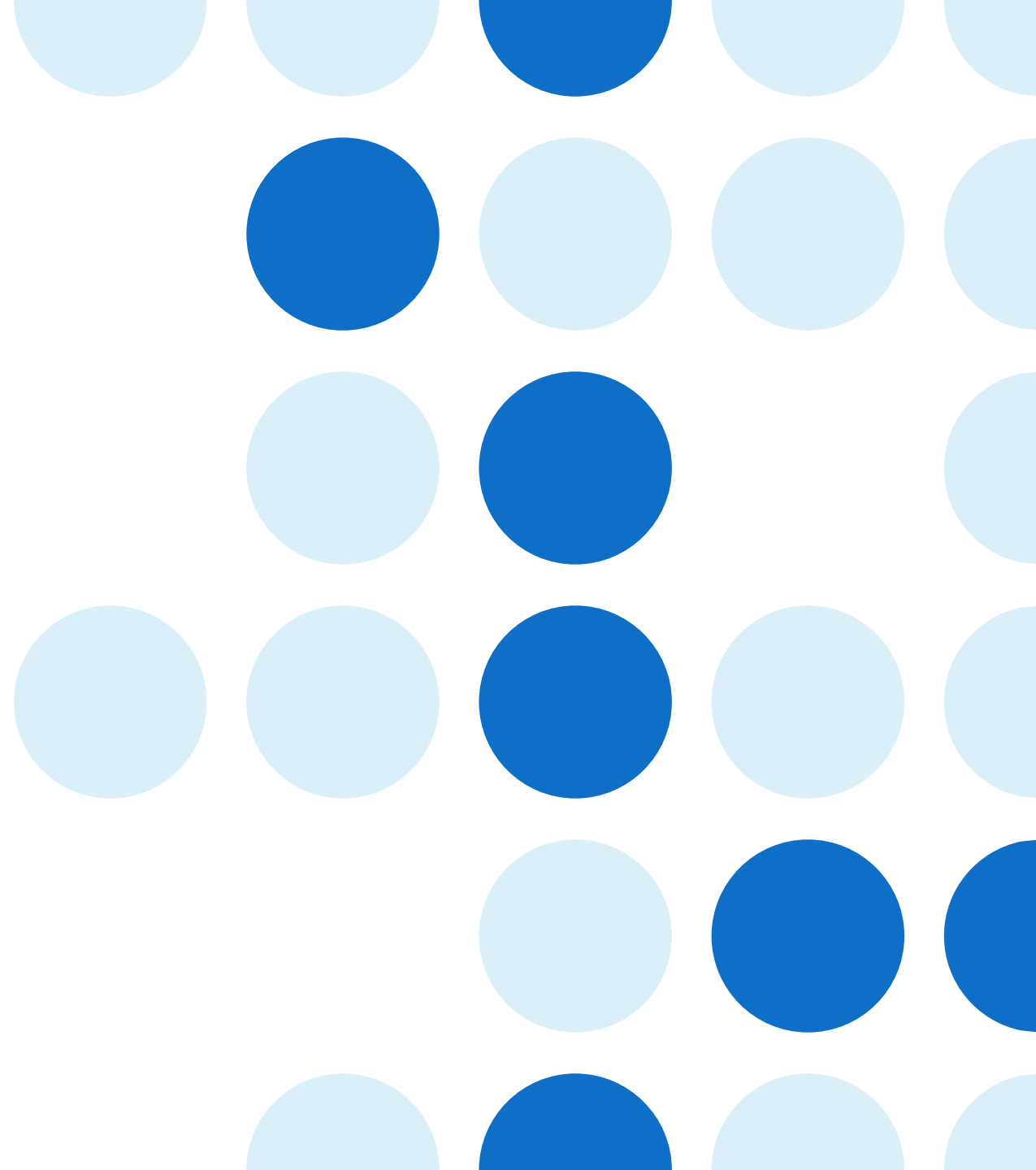
What You Should Be Doing Now

- ***The most important thing you can do to be compliant AND secure is to create a culture of cybersecurity.***
 - Tone at the top is EVERYTHING
 - Training – Wizer, DoD CUI training, Insider Threat Training, Toolbox talks, training together. Everyone should know what their cybersecurity responsibilities are.
 - *Person responsible for cyber in your organization should report to the President/CEO*
-

What You Should Be Doing Now

Develop a culture of continuous improvement. Cyber threats change rapidly and technology changes rapidly; there is no such thing a “**set and forget.**”

Think of your cybersecurity program like you would any quality management system – ISO 9001, ISO 9001.



What You Should Be Doing Now

- **Don't flow down CUI to your subs/suppliers unless it's absolutely necessary**
- Push back on primes/DoD if they flow down CUI unnecessarily

We are all in learning mode, so we must *create a culture of collaboration* with subs/suppliers/primes/DoD.



DOCUMENT EVERYTHING –
your cybersecurity program
should be a quality management
system for cybersecurity.



“If it’s not documented, it didn’t
happen.” Documentation is a
proxy for security.

What You Should Be Doing Now

Assign a Project Manager

- Developing your cybersecurity program should be handled like any project, so assign the responsibility and the authority to someone in your organization - or hire a consultant.
 - Don't wait for a cyber incident...
-



What You Should Be Doing Now

Perform asset inventories. You can't protect what you don't know you have.

Data inventory

Software inventory

Hardware inventory

Data flow diagrams

Network diagrams

Physical security, including diagrams

Personnel security – background checks

What You Should Be Doing Now

- **Minimize your scope** – creating an enclave (segmentation) is a good option

Scope = Risk = \$\$\$

- **Avoid/Reduce CUI** in your environment
 - Snail mail
 - Work with contracting officer/prime to minimize flow down of CUI
 - Keep CUI off your network

CUI = Risk = \$\$\$

What You Should Be Doing Now

Perform a self-assessment using NIST SP 800-171A (320 assessment objectives)

Used DoD Assessment Methodology to calculate score

Have POAMs in place for unimplemented assessment objectives

Put score in the Supplier Performance Risk System

What Does “Implement Security Controls” Mean?

That you have implemented **all** the assessment objectives in each security control and have documented evidence for each objective. There are 320 assessment objectives in the 110 controls in NIST SP 800-171A.

Example:

3.1.3	SECURITY REQUIREMENT Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE <i>Determine if:</i>
3.1.3[a]	<i>information flow control policies are defined.</i>
3.1.3[b]	<i>methods and enforcement mechanisms for controlling the flow of CUI are defined.</i>
3.1.3[c]	<i>designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.</i>
3.1.3[d]	<i>authorizations for controlling the flow of CUI are defined.</i>
3.1.3[e]	<i>approved authorizations for controlling the flow of CUI are enforced.</i>
	POTENTIAL ASSESSMENT METHODS AND OBJECTS <u>Examine:</u> [SELECT FROM: Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. <u>Interview:</u> [SELECT FROM: System or network administrators; personnel with information security responsibilities; system developers]. <u>Test:</u> [SELECT FROM: Mechanisms implementing information flow enforcement policy].

Recommend never using N/A for any control. You can implement those controls via policy.

FIGURE 1: ASSESSMENT PROCEDURE FOR CUI SECURITY REQUIREMENT

How to Perform an Accurate Self-Assessment

Assess to each assessment objective in every control and have documented proof for each objective.

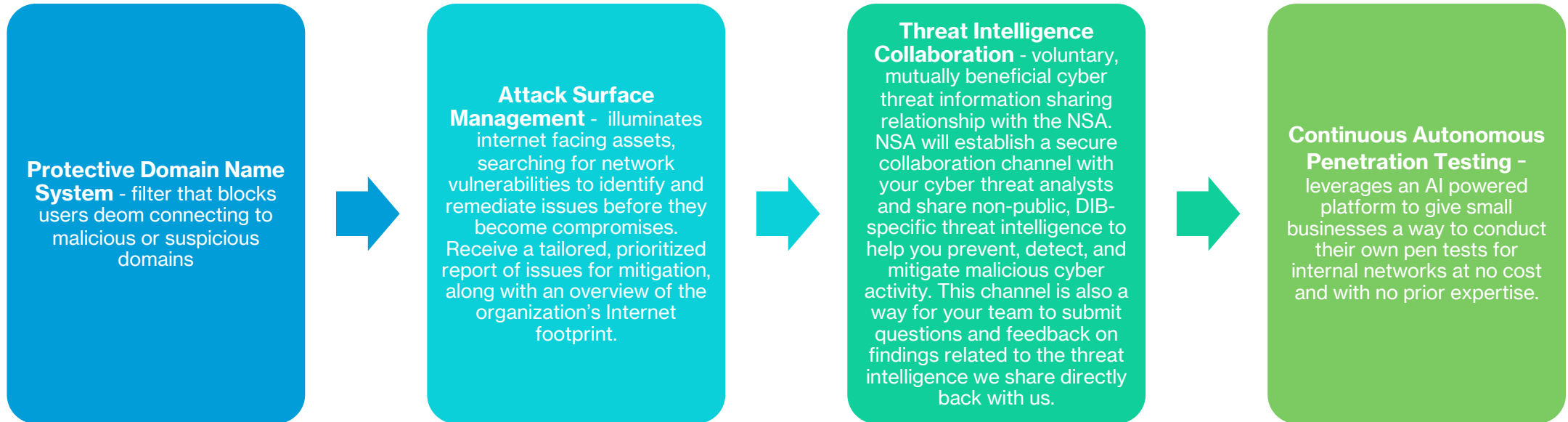
- CMMC Level 1: 59 assessment objectives. If you haven't implemented an objective, you report "Fail" (no scoring or POAMs for CMMC Level 1). If CMMC isn't in your contract, work on implementing the objective(s) ASAP.
- CMMC Level 2: 320 assessment objectives. Controls are worth either 5, 3, or 1 point (DoD Assessment Methodology); subtract the value of unimplemented control from 110; may not take credit for a control unless ALL assessment objectives are met.

NOTE #1: You must have a complete and accurate system security plan (documented) before you upload your score to SPRS. (CMMC Level 2)

NOTE #2: Your self-assessment score is not accurate if you didn't perform comprehensive asset inventories of data, software, and IT hardware/firmware.



What you Should be Doing Now: Contact NSA for Free Tools and Services for Defense Contractors



What you Should be Doing Now: Contact DC3-DCISE for Free Tools and Services for Defense Contractors

- **Cybersecurity as a Service (Caas) Offerings**

- Cyber Resilience Analysis (CRA): evaluates processes and practices across 10-security domains and provides insight into an organization's operational resilience and ability to manage cyber attacks.
 - DCISE3: automated threat detection, scoring, and blocking solution with integration of DCISE threat intelligence.
 - Adversary Emulation (AE): simulates real-world attacker techniques to assess the resilience of your defenses. Includes network mapping, vulnerability assessments, phishing simulations, and web application testing, providing a focused and actionable roadmap for improving security posture.
 - DIB-Vulnerability Disclosure Program: utilizes independent white hat hackers to help you discover vulnerabilities on your publicly facing infrastructure.
-

What You Should Be Doing Now

- Develop an implementation strategy
 - Less expensive controls first?
 - Controls that just require policies/procedures first?
 - Implement controls with highest score value first?

Recommendation: begin with training – CUI, Insider Threat, Wizer-Training, then move to concrete (vs. abstract) controls such as physical protection, personnel security, and media protection.



DoD Assessment Methodology

NIST 800-171 & NIST 800-171A

AC	AT	AU	CM	IA	IR	MA	MP	PS	PP	RA	SA	SC	SI
3.1.1*	3.2.1	3.3.1	3.4.1	3.5.1*	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1*	3.11.1	3.12.1	3.13.1*	3.14.1*
3.1.2*	3.2.2	3.3.2	3.4.2	3.5.2*	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2*
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3*		3.10.3*	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4*		3.12.4	3.13.4	3.14.4*
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5*			3.13.5*	3.14.5*
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20*													
3.1.21													
3.1.22*													

Must Do (SSP)	5	5 or 3	3	1	* FAR 52.204.21 /CMMC Level 1
---------------	---	--------	---	---	-------------------------------

NIST SP 800-171 rev2 Summary

AC	AT	AU	CM	IA	IR	MT	MP	PS	PE	RA	CA	SC	SI
3.1.1	3.2.1	3.3.1	3.4.1	3.5.1	3.6.1	3.7.1	3.8.1	3.9.1	3.10.1	3.11.1	3.12.1	3.13.1	3.14.1
3.1.2	3.2.2	3.3.2	3.4.2	3.5.2	3.6.2	3.7.2	3.8.2	3.9.2	3.10.2	3.11.2	3.12.2	3.13.2	3.14.2
3.1.3	3.2.3	3.3.3	3.4.3	3.5.3	3.6.3	3.7.3	3.8.3		3.10.3	3.11.3	3.12.3	3.13.3	3.14.3
3.1.4		3.3.4	3.4.4	3.5.4		3.7.4	3.8.4		3.10.4		3.12.4	3.13.4	3.14.4
3.1.5		3.3.5	3.4.5	3.5.5		3.7.5	3.8.5		3.10.5			3.13.5	3.14.5
3.1.6		3.3.6	3.4.6	3.5.6		3.7.6	3.8.6		3.10.6			3.13.6	3.14.6
3.1.7		3.3.7	3.4.7	3.5.7			3.8.7					3.13.7	3.14.7
3.1.8		3.3.8	3.4.8	3.5.8			3.8.8					3.13.8	
3.1.9		3.3.9	3.4.9	3.5.9			3.8.9					3.13.9	
3.1.10				3.5.10								3.13.10	
3.1.11				3.5.11								3.13.11	
3.1.12												3.13.12	
3.1.13												3.13.13	
3.1.14												3.13.14	
3.1.15												3.13.15	
3.1.16												3.13.16	
3.1.17													
3.1.18													
3.1.19													
3.1.20													
3.1.21													
3.1.22													

 Administrative (e.g., policies, standards & procedures)

 Technical Configurations(e.g., security settings)

 Software Solution

 Hardware Solution

 Software or Hardware Solution

 Assigned Tasks To Cybersecurity Personnel

 Assigned Tasks To IT Personnel

 Assigned Tasks To Application/Asset/Process Owner

 Configuration or Software Solution

 Configuration or Software or Hardware or Outsourced Solution

What You Should Be Doing Now



Work with your MSP/MSSP on CMMC compliance. If your service provider handles your FCI/CUI they are in scope to your assessment, and you “inherit” controls from them.



Work with you cloud service providers. If they store, transmit, or process CUI they must be FedRAMP Moderate Baseline *Authorized*.

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	15 required by FAR clause 52.204-21	- Conducted by Organization Seeking Assessment (OSA) annually - Results entered into the Supplier Performance Risk System (SPRS)	Not permitted	- After each assessment - Entered into SPRS
Level 2 (Self)	110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	- Conducted by OSA every 3 years - Results entered into SPRS - CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	- Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days - Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	- After each assessment and annually thereafter - Assessment will lapse upon failure to annually affirm - Entered into SPRS
Level 2 (C3PAO)	110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	- Conducted by C3PAO every 3 years - Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) - CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	- Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days - Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	- After each assessment and annually thereafter - Assessment will lapse upon failure to annually affirm - Entered into SPRS
Level 3 (DIBCAC)	110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	- Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment - Conducted by DIBCAC every 3 years - Results entered into CMMC eMASS - CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	- Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days - Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	- After each assessment and annually thereafter - Assessment will lapse upon failure to annually affirm - Level 2 (C3PAO) affirmation must also continue to be completed annually - Entered into SPRS

Key Change to the CMMC Program

External Service Providers (ESP) such as managed service providers/managed security service providers that handle FCI/CUI do not need a CMMC certification, but they are considered **in-scope to your CMMC assessment**; their services must be documented in your System Security Plan if they handle CUI.

Since you “inherit” NIST SP 800-171 controls from your ESP, they must provide a shared responsibility matrix showing which of the 320 assessment objectives they implement on your behalf and how they implement them.

Remember the rest of DFARS

252.204-7012

- (3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures....may be required to provide adequate security in a dynamic environment or to accommodate special circumstances...
 - Cyber incident reporting requirement
 - Conduct review to determine if sensitive data has been compromised
 - Report cyber incidents to the DoD at <https://dod.mil> (NOT KO, CISA, FBI, etc.)
 - Acquire a DoD-approved Medium Assurance Certificate to report cyber incidents - <https://public.cyber.mil/eca/>
 - Submit malicious software to DoD Cyber Crime Center (NOT KO)
 - Flow down the DFARS clause ONLY IF you flow down CUI
-

Resources

- FedRAMP Marketplace - <https://marketplace.fedramp.gov/products>
 - NARA CUI Categories - <https://www.archives.gov/cui>
 - Insider Threat Training - <https://www.cdse.edu/Training/eLearning/INT101/>
 - CUI Training - <https://www.dodcui.mil/Training/>
 - CUI Presentation (ppt) - <https://www.dcsa.mil/Portals/128/Documents/CTP/CUI/DCSA%20CUI%20Training%20Template%20Version%203.pdf>
 - Wizer Cyber Awareness Training - <https://www.wizer-training.com/>
-

Resources

- NSA Tools/Services - <https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/>
 - DC3/DCISE Cybersecurity as a Service Products - [CaaS](#)
 - Medium Assurance Certificate - <https://public.cyber.mil/eca/>
 - CMMC Resources - <https://dodcio.defense.gov/CMMC/Resources/>
 - CMMC FAQs - <https://dodcio.defense.gov/Portals/0/Documents/CMMC/CMMC-FAQs.pdf>
 - Scoping Video - https://www.youtube.com/watch?v=LWuM_IbD_Mo
 - Project Spectrum - <https://www.projectspectrum.io/#/>
-

Final Thoughts

If you have not started your cybersecurity compliance program, you are already way behind. The longer you wait, the more expensive it will be.

Do not misrepresent your cybersecurity posture. (DoJ Civil Cyber Fraud Initiative)

CMMC For Infrastructure Contractors

2025 SE Region Federal Construction/Infrastructure/Environmental Summit

April 24, 2025
