Cyber Thursday:

CMMC – From Top to Bottom – A Program Review

December 18 | 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute

WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

Wisconsin Procurement Institute

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

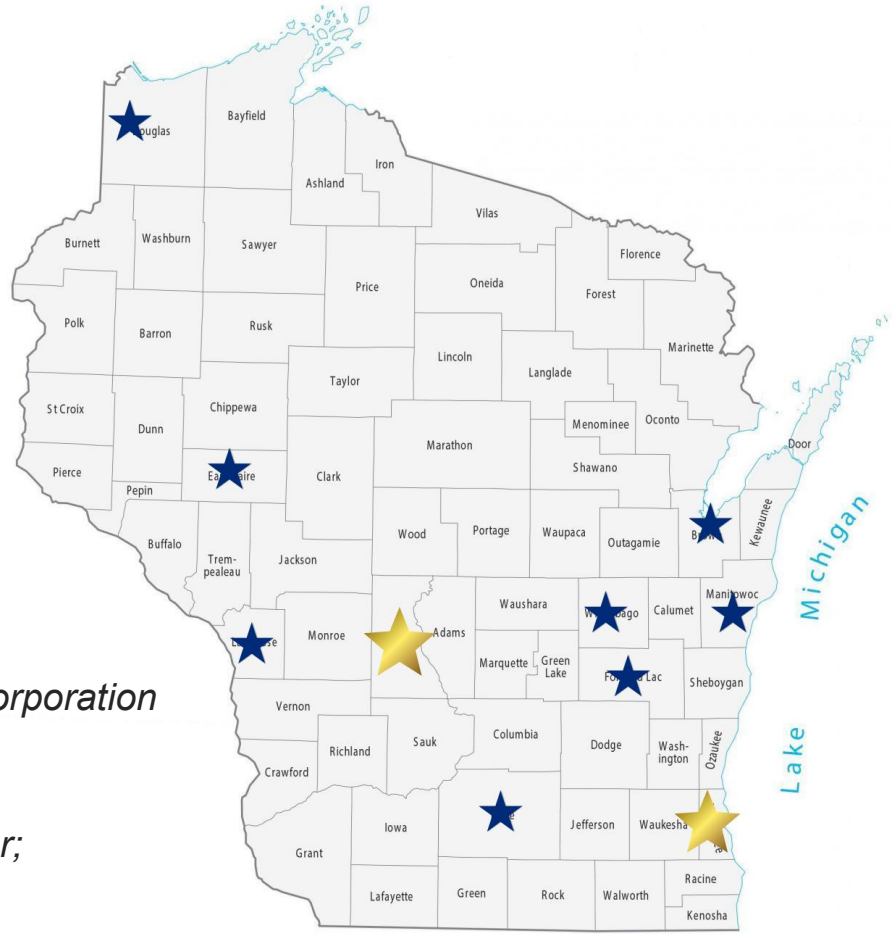
WPI provides services and training to all of Wisconsin's 72 counties

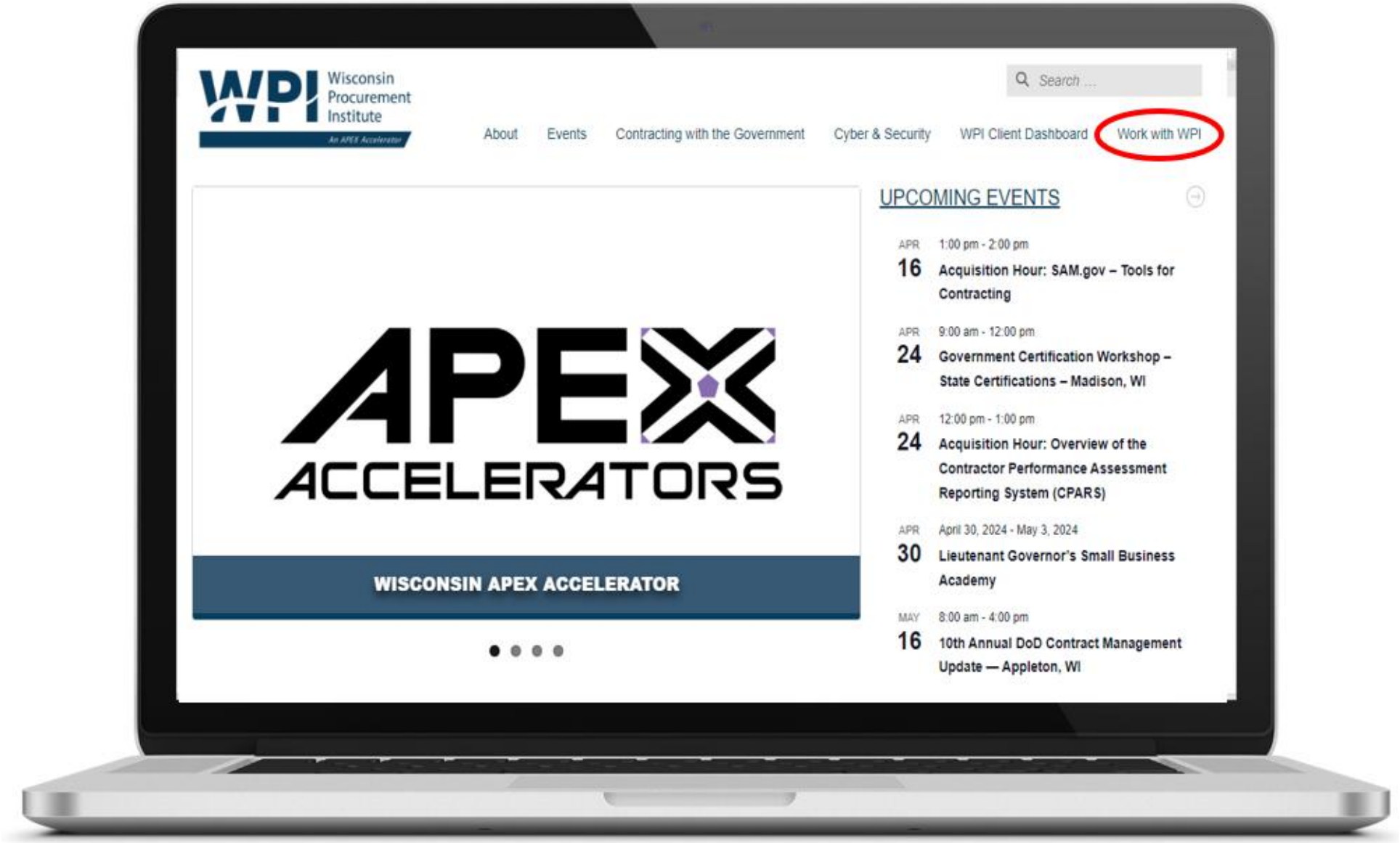
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more……

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*




WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Wisconsin Procurement Institute

An APEX Accelerator

CMMC:

From Top to Bottom

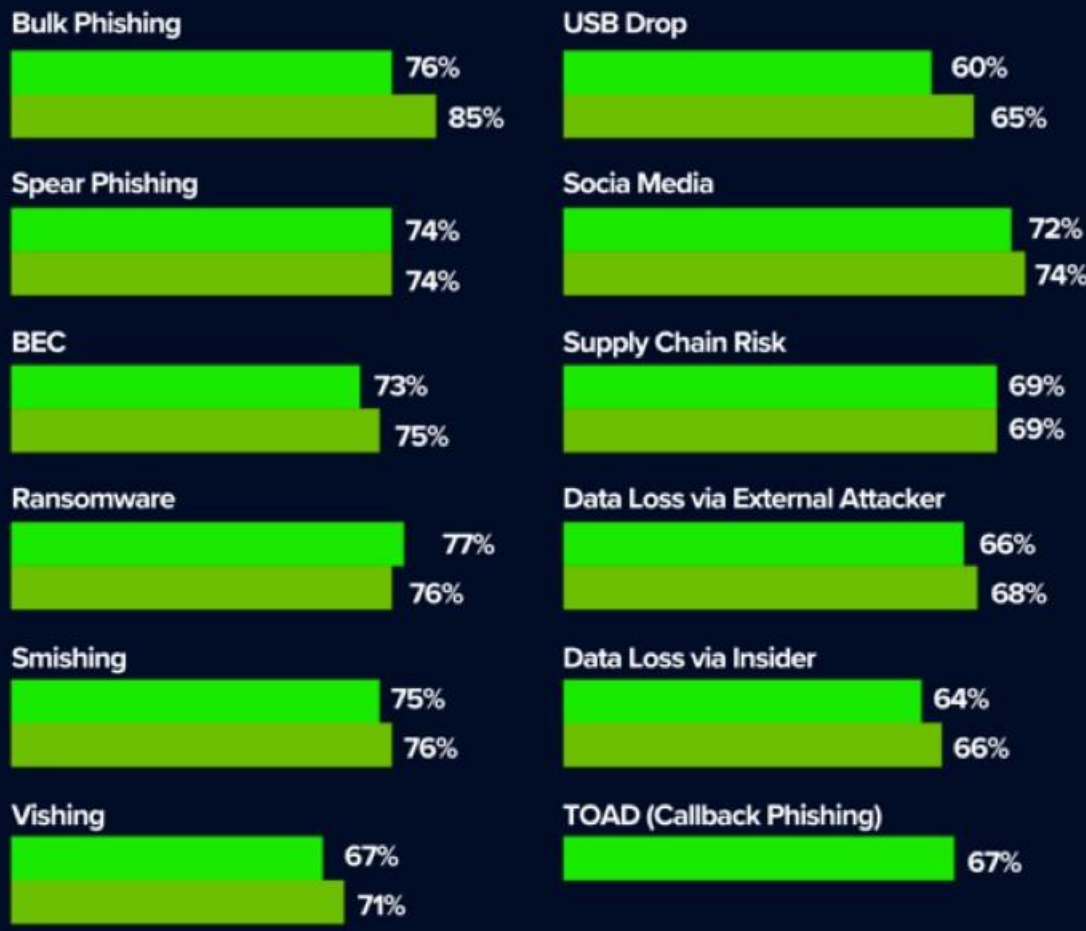
December 18th, 2025

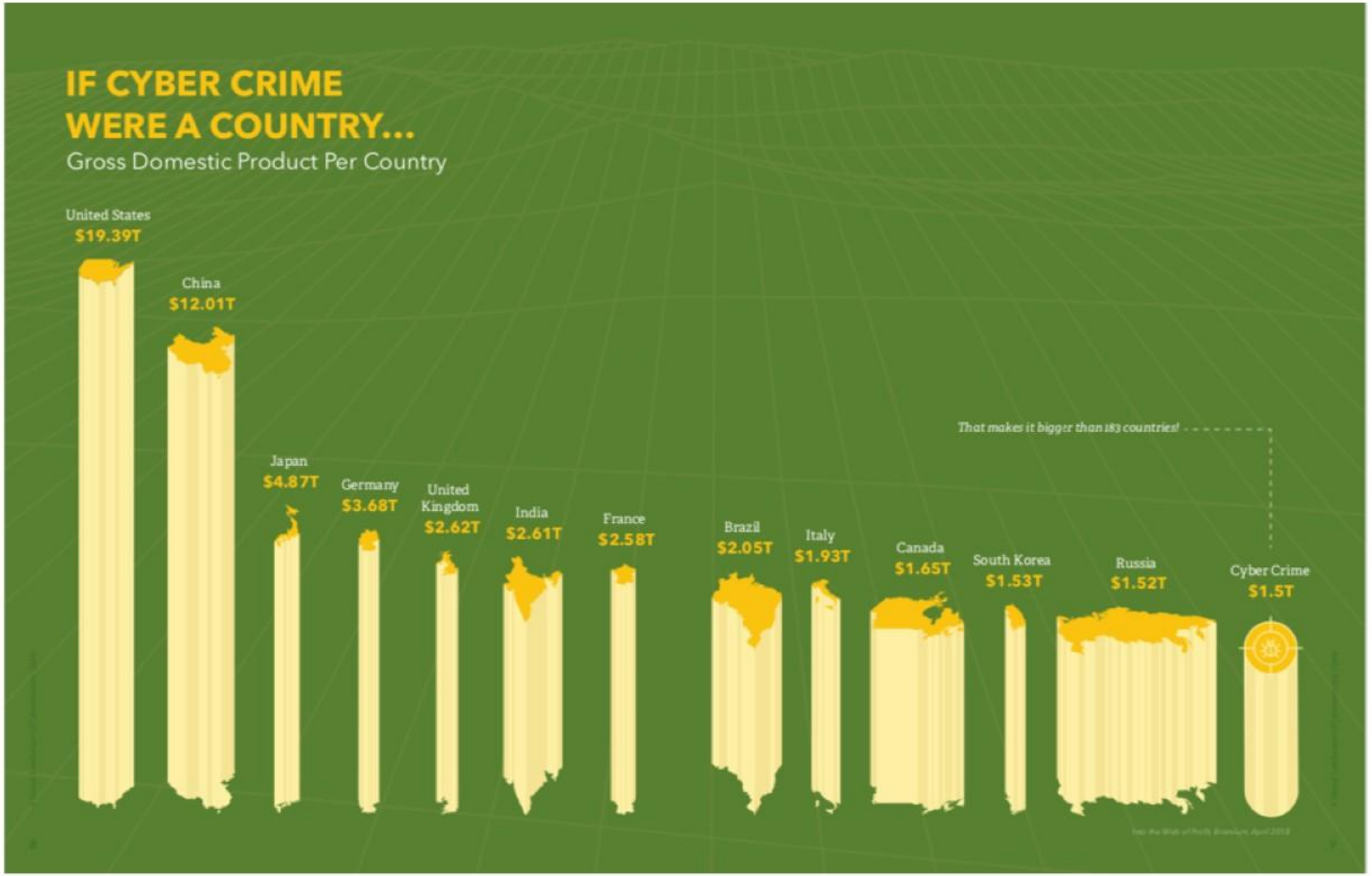

3103

Wow. That escalated quickly! (From Checkpoint)

bright defense

Frequency of Attacks




IF CYBER CRIME
WERE A COUNTRY...
Gross Domestic Product Per Country
United States
$19.39T
China
$12.01T
Japan
$4.87T
Germany
$3.68T
United Kingdom
$2.62T
India
$2.61T
France
$2.58T
Brazil
$2.05T
Italy
$1.93T
Canada
$1.65T
South Korea
$1.53T
Russia
$1.52T
Cyber Crime
$1.5T
That makes it bigger than 183 countries!

Agenda

01 **The Federal Requirements**

02 The Program Elements

03 Assessments and Attestations

Ok, but what is a CFR?

- CFR (Code of Federal Regulations) is a collection of all the general an dpermanent rules and regulations issued by the U.S. federal departments and agencies.

And why mention the 32 CFR?

- The 32 CFR deals specifically with National Defense.
- 32 CFR Part 170 was published October 15, 2024 and formally established the CMMC Program.
- Defined roles and requirements.

Key Points: 32 CFR Part 170

Purpose and Scope

You must meet specified cybersecurity standards if handling FCI and CUI.

Specified Standards and FCI/CUI Requirements

The specified standards are NIST SP 800-171 Rev 2 and NIST SP 800-172.

CMMC Level 1 - FCI
CMMC Level 2 - CUI
CMMC Level 3 - CUI with Advanced Protections

Annual Affirmations and Tiered Implementation

Despite CMMC C3PAO Validations being good for 3 years – companies must still submit annual self-attestations. The C3PAO Assessments will be ramped up, escalating each year, until complete coverage of the DIB at Level 2 is achieved.

ESP

External Service Providers are no longer required to be independently certified – but their systems must be accounted for.

Why the 48 CFR?

- The 48 CFR governs the Federal Acquisition Regulations (FAR) System.

- 32 CFR defined the requirements. 48 CFR now makes it enforceable in actual contracts.

- **Evolving Adversaries; increased use of AI-enabled Tradecraft**
- EO 14028
- OMB M-22-09
- DOD Memo: DoD COTS Information and Communications Technology SCRM

Key Points: EO 14028

Modernize and Move to Zero Trust

Agencies must advance towards a Zero Trust Architecture and plan for cloud migration accordingly.

MFA & Encryption Mandate

All agencies must adopt multi-factor authentication and encrypt data regardless of system designation.

Cyber Safety Review Board

CSRB to review major incidents and recommend fixes.

EDR, SBOMS, etc

Mandates the implementation of more advanced EDR tools and the use of SBOMs, highlighting the importance of software as a key to government systems.

Key Points: OMB M-22-09

Modernize and Move to Zero Trust

Required agencies to meet specific cybersecurity objectives by end of FY 2024.

The Five Pillars

Goals were organized according to the Five Pillars of Zero Trust. Identity, Devices, Networks, Ampplications & Workloads, Data.

Zero Trust Lead

Must be designated within 30 days – submit a plan through FY 2024.

Only Going To Progress

Efforts to harden the DOD and Federal Agencies against Cyber Attacks have been a consistent push from the Executive level of the Federal Government since. 2012.

Key Points: 48 CFR 204, 212, 217 and 252

The New DFARS rule

The final DFARS rule titled "*Asessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)*" was published.

Contractual Clauses Added

The key contractual clause DFARS 252.204-7021 was added.

Flow Down Requirements

Prime contractors must ensure their subcontractors are also appropriately certified.

Phased Rollout of CMMC Begins November 10, 2025

Phase I: Level 1 and 2 self-assessments (November 2025)
Phase II: Level 2 (C3PAO) requirements (November 2026)
Phase III: Level 3 (DIBCAC) requirements (November 2027)

DFARS 252.204-7025 (Notice of Cybersecurity Maturity Model Certification Level Requirements)

The CMMC level required by this solicitation is: _____. This CMMC level or higher (see 32 CFR part 170)is required prior to award for each contractor information system that will process, store, or transmit Federal contract information (FCI) or controlled unclassified information (CUI) during performance of the contract.

Phased Rollout Roadmap

- **Phase I:** Beginning on November 10, 2025 and applies to contracts that will include Level 1 and Level 2 Self-Assessment Levels
- **Phase II:** 12 Months from Phase I, applies to NEW contracts that will include Level 2 C3PAO Requirements
- **Goal:** The DoD wants all DIB Contractors to be certified at their appropriate CMMC Level by End of 2028.

Ahhhhhh, What Do I Do?!

- **Review Existing Contracts:** If your existing contracts have DFARS 252.204-7012, 252.204-7019, or 252.204-7020 – CMMC Level 2 is likely your goal.
- **Talk to your buyers:** If you haven't heard from your primes about CMMC already – you need to start this conversation about what they anticipate you requiring.
- **Get Help and Make a Plan:** You are likely not prepared. Get yourself prepared.

Agenda

01 The Federal Requirements

02 **The Program Elements**

03 Assessments and Attestations

DFARS 252.204-7012

- ❑ The Contractor shall provide adequate security on all covered contractor information systems.
- ❑ The contractor shall implement NIST SP 800-171.

NIST SP 800-171r2

Chapter 3: Page 9 NIST SP 800-171r2

Nonfederal organizations describe, in a system security plan, how the security requirements are met or how organizations plan to meet the requirements and address known and anticipated threats. The system security plan describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems.

Nonfederal organizations develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented.

Organizations can document the system security plan and the plan of action as separate or combined documents and in any chosen format.

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

1. NIST Special Publication 800-18 Revision 1
   NIST Special Publication 800-18 Revision 1
   Guide for Developing Security Plans for Federal Information Systems
2. NIST SP 800-171r2
   NIST Special Publication 800-171r2
   Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
3. NIST SP 800-171A
   NIST Special Publication 800-171A
   Assessing Security Requirements for Controlled Unclassified Information

System Security Plan

- Living Document
- Plan of Actions and Milestones (POAM)
- Defines Categorization for the Information System
- Provides an Overview of the Security Requirements for the information system
- Describes the Security Controls in place for those requirements

System Information

System Name and Identifier

Each system should be assigned a name and unique identifier. This should remain the same throughout the life of the system.

System Categorization

System must be categorized in accordance using FIPS 199.

NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories

ASSESSMENT OBJECTS

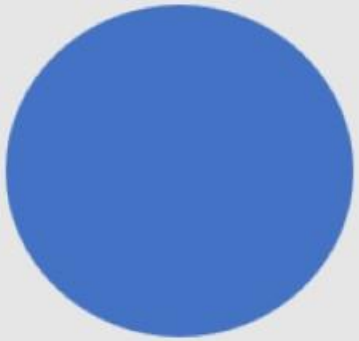
Identify specific items being assessed and can include specifications, mechanisms, activities, and individuals.

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

Scoping the Information System

System Boundaries

- ❑ Under the same direct management control
- ❑ Have the same function or objective
- ❑ Same characteristics or security needs
- ❑ Reside in the same general operating environment



Major Applications

- ❑ Requires special attention due to importance to mission
- ❑ High Development, Operating, or maintenance costs
- ❑ Can compromise multiple programs, hardware, software, and telecom components.
- ❑ Explains Cyber Risks

General Support Systems

- ❑ Interconnected set of resources under the same management control that shares common functionality.
- ❑ LAN, Backbone, Com Network, Data Processing Center, etc.

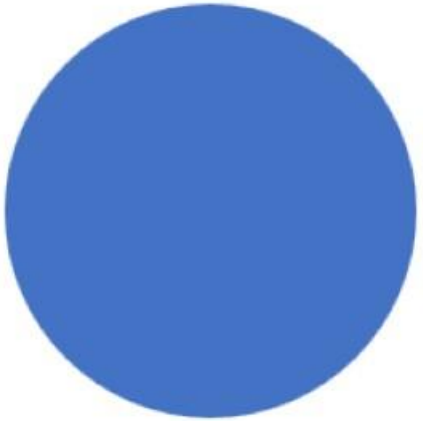
Minor Applications

- ❑ Typically secured by system in which it resides
- ❑ Of low importance or use
- ❑ May or may not interact with CUI

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*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]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

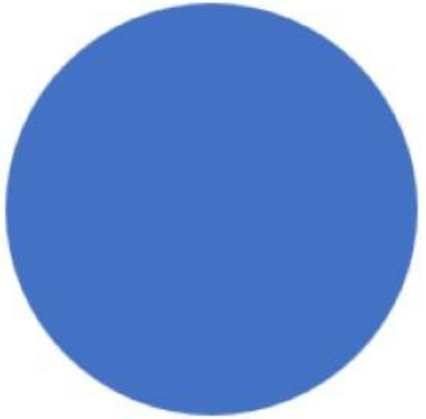
Plan of Action and Milestones

Tasks that need to be accomplished



Milestones for meeting the tasks

Resources required to accomplish the elements of the plan



Scheduled completion dates for the milestones

NIST Control Number	Control	Responsible Office	Scheduled Completion Date	Milestones with Interim Completion Dates
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).			
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.			
3.1.3	Control the flow of CUI in accordance with approved authorizations.	ISO - John Johnston	Jun-23	Draw Business Process Flow, Update Employee Handbook, Draft Acceptable Use Policy. Review Service Accounts and ensure Alpha and Bravo account activity is correctly logged.

Agenda

01 The Federal Requirements

02 The Program Elements

03 **Assessments and Attestations**

NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

1. NIST Handbook 162
   NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements
2. NIST SP 800-171A
   NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information
3. DoD Memo
   DoD Memo
   DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements

Internal Documentation

System Security Plan

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Security Training

Training documentation provided to employees to improve their ability to respond to cyber attacks and protect confidential information.

Incident Response

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).

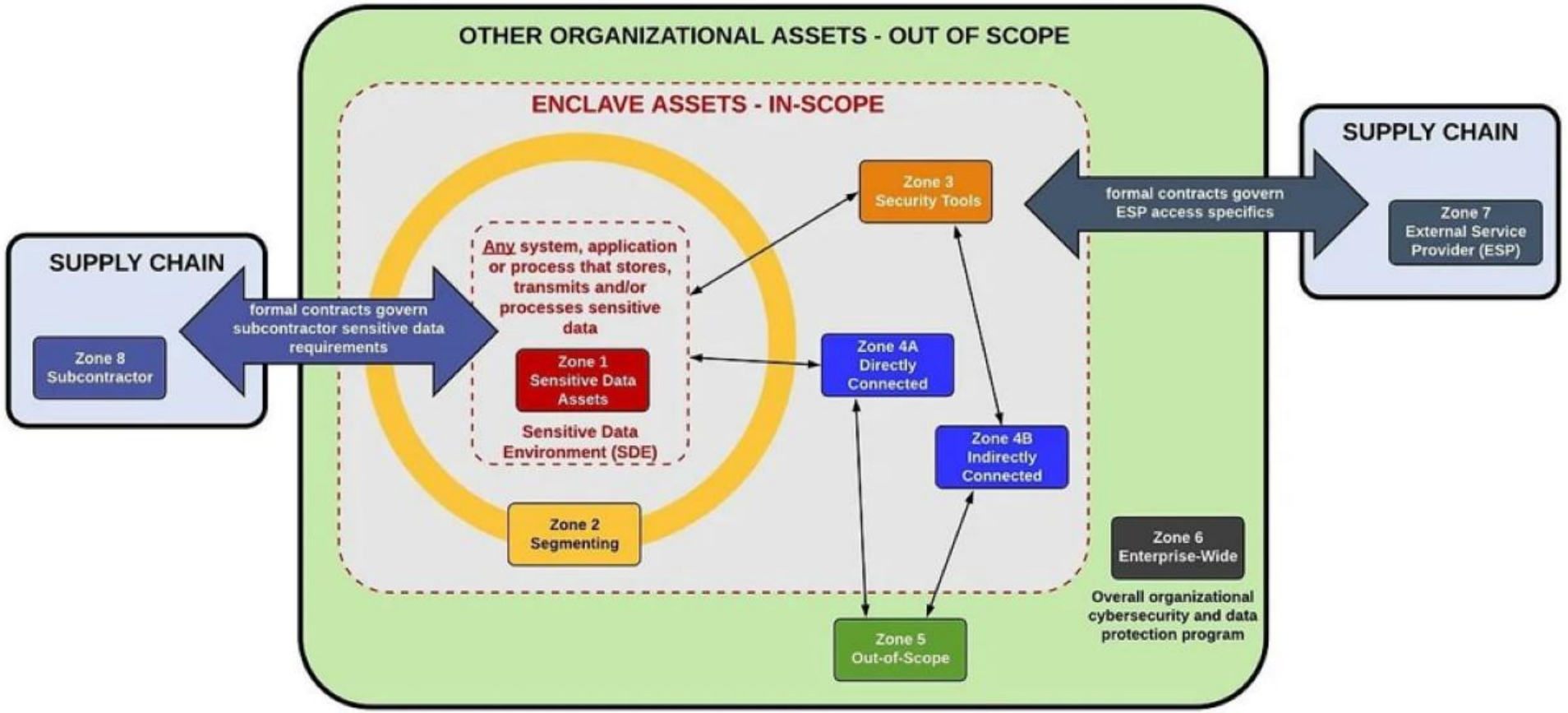
Prior Assessments

Previously conducted assessments.

Additional Internal Documents

- Business Continuity Plans
- Disaster Recovery Plans
- Plan of Action and Milestones
- Acceptable Use Plan
- Business Process Flow
- Network Diagram

SCOPING THE ASSESSMENT



INFORMATION

- CUI (Drawings, Parts Lists)
- FCI (Contracts, RFQs)
- EAR/ITAR

SECURITY ASSETS

- Digital Hardware
- Software
- Cloud Services

PRINTED MATERIAL

- Job Travelers
- Diagrams & Drawings
- Work Instructions / TO's

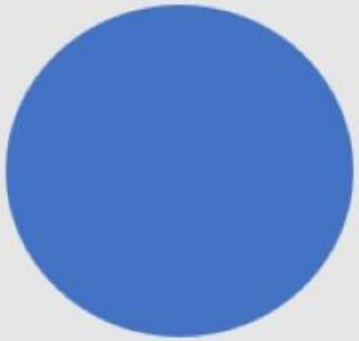
PERSONNEL

- U.S Persons
- Principle of Least Privilege

Who Performs the Assessment?

System Owner

- ❑ Ensures Cooperation
- ❑ Identifying Key Individuals
- ❑ Identifying Delegated Responsibilities
- ❑ Identifying Business Priorities



IT Manager

- ❑ Technical Expertise
- ❑ Defines Implementation
- ❑ Identifies Technical Shortfalls
- ❑ Explains Cyber Risks

Security Officer

- ❑ Determines whether Control is adequately met
- ❑ Defines Control Requirements
- ❑ Identifies Procedural Shortfalls

Operations Manager

- ❑ Defines work flow.
- ❑ Highlights use of applications.
- ❑ Explains operational needs and challenges

ASSESSMENT OBJECTIVES

Includes a determination statement related to the CUI security requirement that is the subject of the assessment.

Ex. 3.1.3 Control the flow of CUI in accordance with approved authorizations

ASSESSMENT METHODS

Define the nature and the extent of the assessor's actions. They include **examine**, **interview**, and **test**.

Ex. 3.1.3 Examine architectural solutions to control flow of system data.

ASSESSMENT OBJECTS

Identify specific items being assessed and can include specifications, mechanisms, activities, and individuals.

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

Assessment Process

Assess each of the NIST SP 800-171 controls using the NIST SP 800-171A to ensure all audit points are covered.

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*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]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

3.1.3 Control the flow of CUI in accordance with approved authorizations.

Do you have architectural solutions to control the flow of system data?

Yes No Partially Does Not Apply Alternative Approach

Do you document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The solutions may include firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who is allowed to access the information) without explicit regard to subsequent accesses to that information.

Examples of flow control restrictions include:

- keeping export-controlled information from being transmitted in the clear to the internet,
- blocking outside traffic that claims to be from within the organization,
- restricting web requests to the internet that are not from the internal web proxy server, and
- limiting information transfers between organizations based on data structures and content.

Where to Look:

- access control policy
- information flow control policies
- procedures addressing information flow enforcement
- information system design documentation
- information system configuration settings and associated documentation
- information system baseline configuration
- list of information flow authorizations information system audit records
- other relevant documents or records

Who to Talk to:

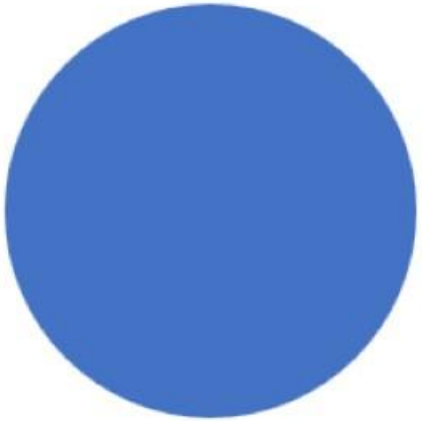
- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

- automated mechanisms implementing information flow enforcement policy

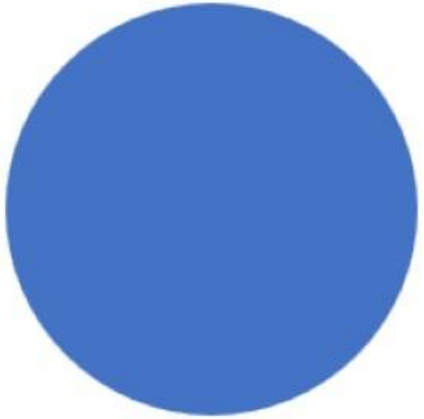
NIST SP 800-171 Summary Score

NIST SP 800-171 can assign 5, 3, or 1 points per control.



NIST Summary Score can range from a -203 to 110.

There is no partial credit for a control. Either all objectives are met or **NO** points are awarded.



NIST Summary Score must be submitted in SPRS. Cannot be viewed by non-government entities.

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

DOCUMENT HEADINGS

Department of Defense
Office of the Secretary
32 CFR Part 170
[Docket ID: DoD-2023-OS-0063]
RIN 0790-AL49

1

CMMC Program

For verifying contractors have implemented security measures for FCI and CUI.

2

Tiered Implementation

Year 1: 135 Assessments
Year 2: 673 Assessments
Year 3: 2,252 Assessments
Year 4: 4,452 Assessments

3

Final Requirements

Level 1
Level 2 (Self)
Level 2 (C3PAO)
Level 3 (DIBCAC)

WPI Wisconsin Procurement Institute

APEX ACCELERATORS

Choosing a Level

CMMC Level Selection

An OSA will select the CMMC level it desires to attain. Once the CMMC Program is implemented, a DoD solicitation will specify the minimum CMMC Status required to be eligible for award. One of four CMMC Statuses will be specified:

OSA – Organization Seeking Assessment

CMMC Levels and Requirements

TABLE 1—CMMC LEVEL AND ASSESSMENT REQUIREMENTS

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 SPRS (or its successor capability).	• 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 (or its successor capability). • 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 (or its successor capability).
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) (or its successor capability). • 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 (or its successor capability).
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 Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every 3 years. • Results entered into CMMC eMASS (or its successor capability). • 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 (or its successor capability).

Supplier Performance Risk System

- ❑ **Level 1**
- ❑ Level 2 (Self)
- ❑ Level 2 (C3PAO)
- ❑ Level 3

Level 2 (Self)

Level 2 (Self) is a **self-assessment** to secure CUI processed, stored, or transmitted in the course of fulfilling the contract. The OSA must comply with the 110 Level 2 security requirements derived from **NIST SP 800-171 R2**.

Level 2 (C3PAO)

Level 2 (C3PAO) differs from Level 2 (Self) in the method of verifying compliance. OSAs **must hire a C3PAO** to conduct an assessment of the OSA's compliance with the 110 security requirements of **NIST SP 800-171 R2**. OSAs can shop for C3PAOs on the CMMC Accreditation Body (AB) Marketplace.

If the overall scoring of the Assessment after placing eligible items on the Limited Practice Deficiency Correction program results in **less than 80%** (88/110 practices "MET"), the OSC will receive a final finding of "Not Achieved" for CMMC Level 2 Certification. The OSC will be required to correct deficiencies and reapply for CMMC L2 Certification.

If the overall scoring of the Assessment after placing items on the Limited Practice Deficiency Correction program results in **greater than or equal to 80%** (88/110 practices "MET"), the OSC will be required to correct deficiencies.

THE CYBER AB

CMMC CERTIFICATION

ABOUT US ▾ ACCREDITATION ▾ RESOURCES ▾ CMMC ECOSYSTEM ▾ NEWS & EVENTS ▾ MARKETPLACE CAICO

www.cyberab.org

Wisconsin Procurement Institute

An APEX Accelerator

Matthew Frost

mattf@wispro.org

APEX ACCELERATORS

Acquisition Hour

The Acquisition Hour webinar series covers a range of topics from market entry, sales growth, small business certifications, compliance, and more. Attendees receive 1 CPE credit for attending.

- **January 14** – Selling to the Government – Is There an Opportunity for Your Small Business?
- **January 21** – The Basics of Cybersecurity for Any Small Business
- **February 11** – Is the GSA Schedule Right for Your Business?
- **February 18** – Overview of the Contractor Performance Assessment Reporting System (CPARS)

…More information and registrations at wispro.org/events

Cyber Thursday

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **December 18** – CMMC – From Top to Bottom – A Program Review
- **January 22** – CMMC: Correctly Scoping Your Environment
- **February 26** – CMMC: Control Set Series: 3.1 Access Control
- **March 26** – CMMC: Control Set Series: 3.2 Awareness and Training
- **April 30** – CMMC: Control Set Series: 3.3 Audit and Accountability
- **May 28** – CMMC: Control Set Series: 3.4 Configuration Management

…More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

December 18 2025

This webinar is eligible for

1 CPE credit

To receive a certificate of completion, contact apexaccelerator@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MatthewF@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226