Cyber Thursday:

Federal Cyber Update – a Review of current regulations in effect and where they stand

November 20 | 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.

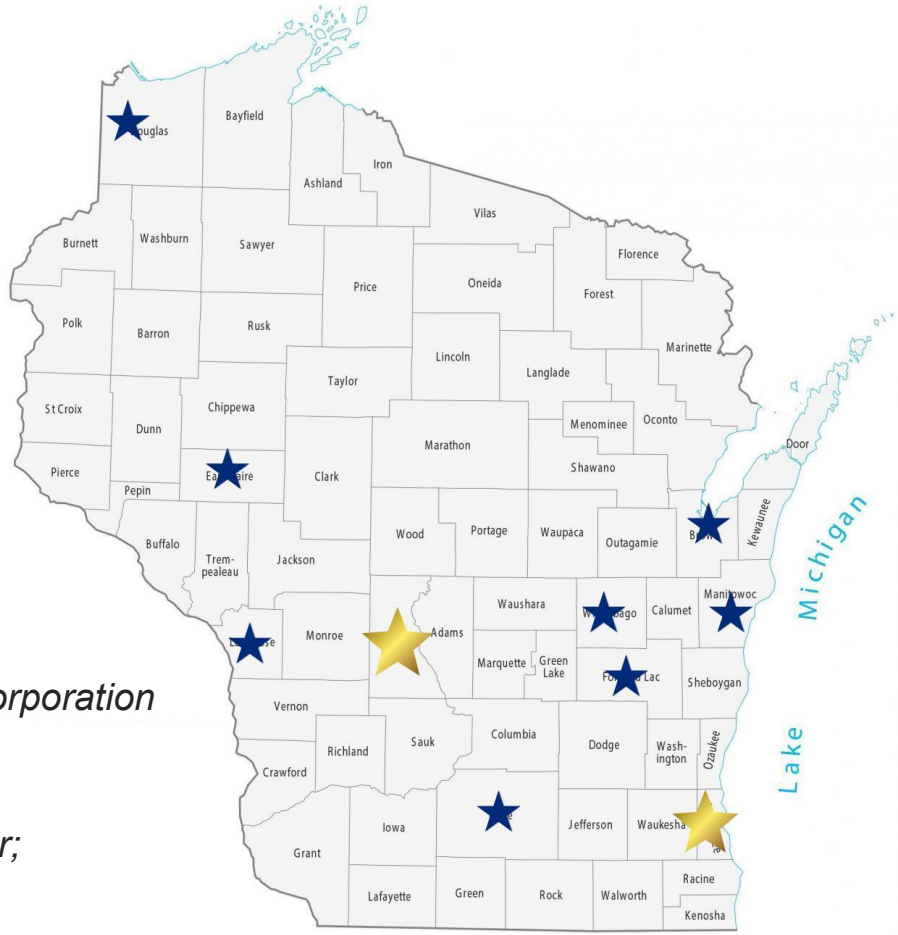
WPI provides services and training to all of Wisconsin's 72 counties

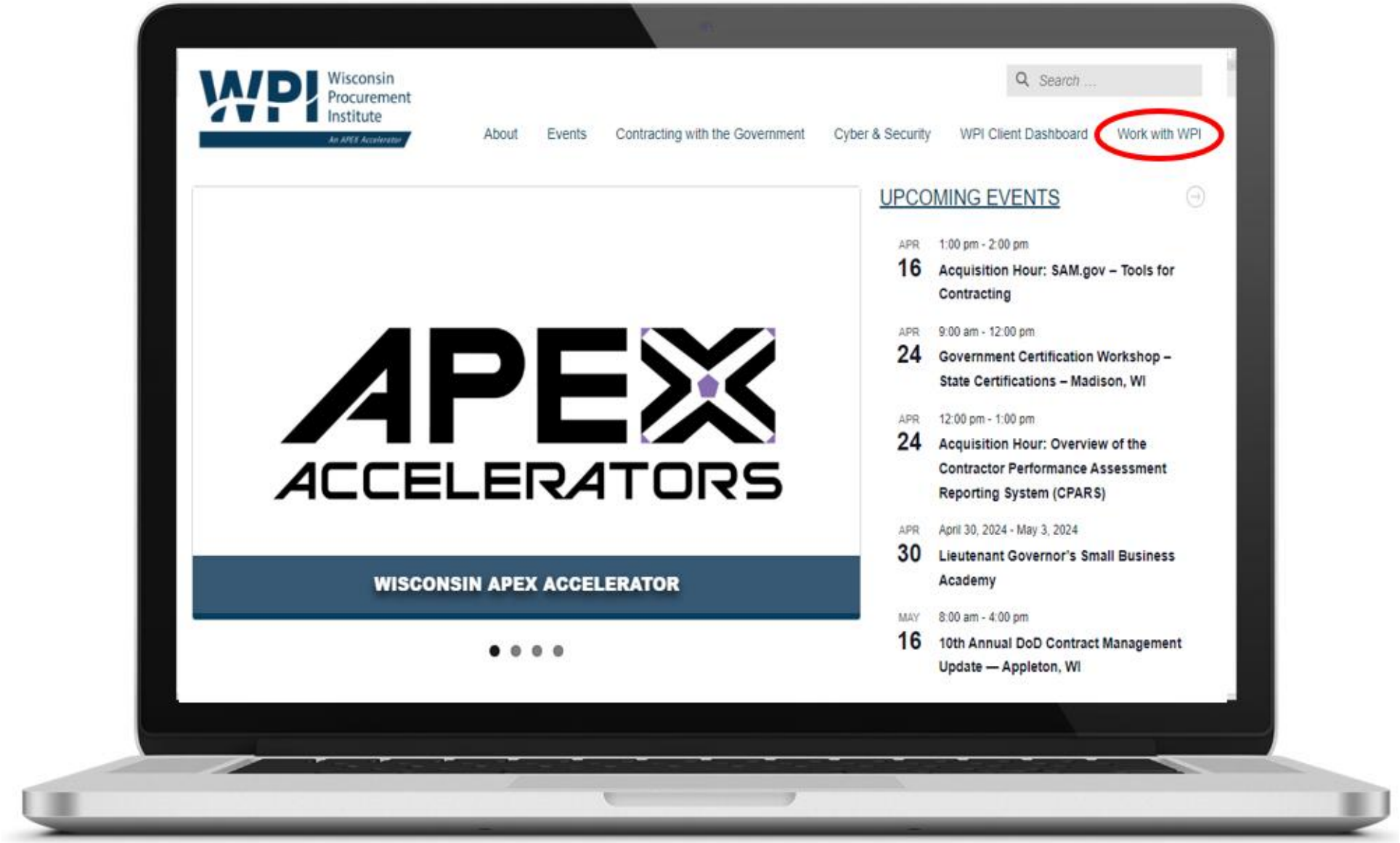
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting 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

Federal Cyber Update: A Review of Current Regulations

November 20th, 2025

Agenda

01 **The Federal Position on Zero Trust**

02 FAR, DFARS, CMMC, and still more Acronyms

03 Foreign Ownership, Control, or Influence (FOCI – another acronym)

Why Now?

- **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.

ExecutiveGov

KATIE ARRINGTON

Performing the Duties of
Chief Information Officer

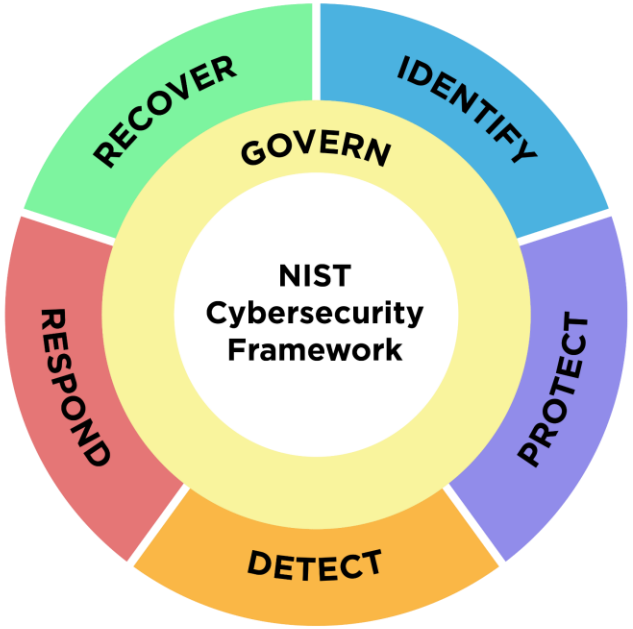
Department of Defense


LOCKHEED MARTIN
3103

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



1

NIST CSF 2.0

NIST Cybersecurity Framework (CSF) 2.0 – Mar 2025

2

CISA Implementation Report

CISA Zero Trust Architecture Implementation Report – Jan 2025

3

OMB M – 25 - 04

FY25 FISMA Guidance – pushing Zero Trust Maturity progress through 2025, aligning ZT Implementation with NIST CSF 2.0

Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

Five Pillars:

Identity, Devices, Networks, Applications & Workloads, Data

The Alignment

National Institute of Standards and Technology

NIST SP 800-207

Zero Trust Architecture

NIST CSF 2.0

NIST CSF is being leveraged by the Federal Government as a governance methodology that includes the management and oversight of ZT Implementation.

ZT is now a tactical doctrine for how information systems are to be evaluated and secured.

Summary of Zero Trust Roadmap

- **Baseline:** Inventory, Identity Consolidation, Endpoint EDR, Logging
- **Build:** Risk-Based Access, Device Posture Gating, App-Level Authorization, Data Labeling
- **Scale:** Automation (SOAR), Continuous Verification, Policy-As-Code, Microsegmentation
- **Optimize:** Enterprise-wide Observability, Automated least-privilege, continuous ATO

Agenda

01 The Federal Position on Zero Trust

02 **FAR, DFARS, CMMC, and still more Acronyms**

03 Foreign Ownership, Control, or Influence
(FOCI – another acronym)

Regulations

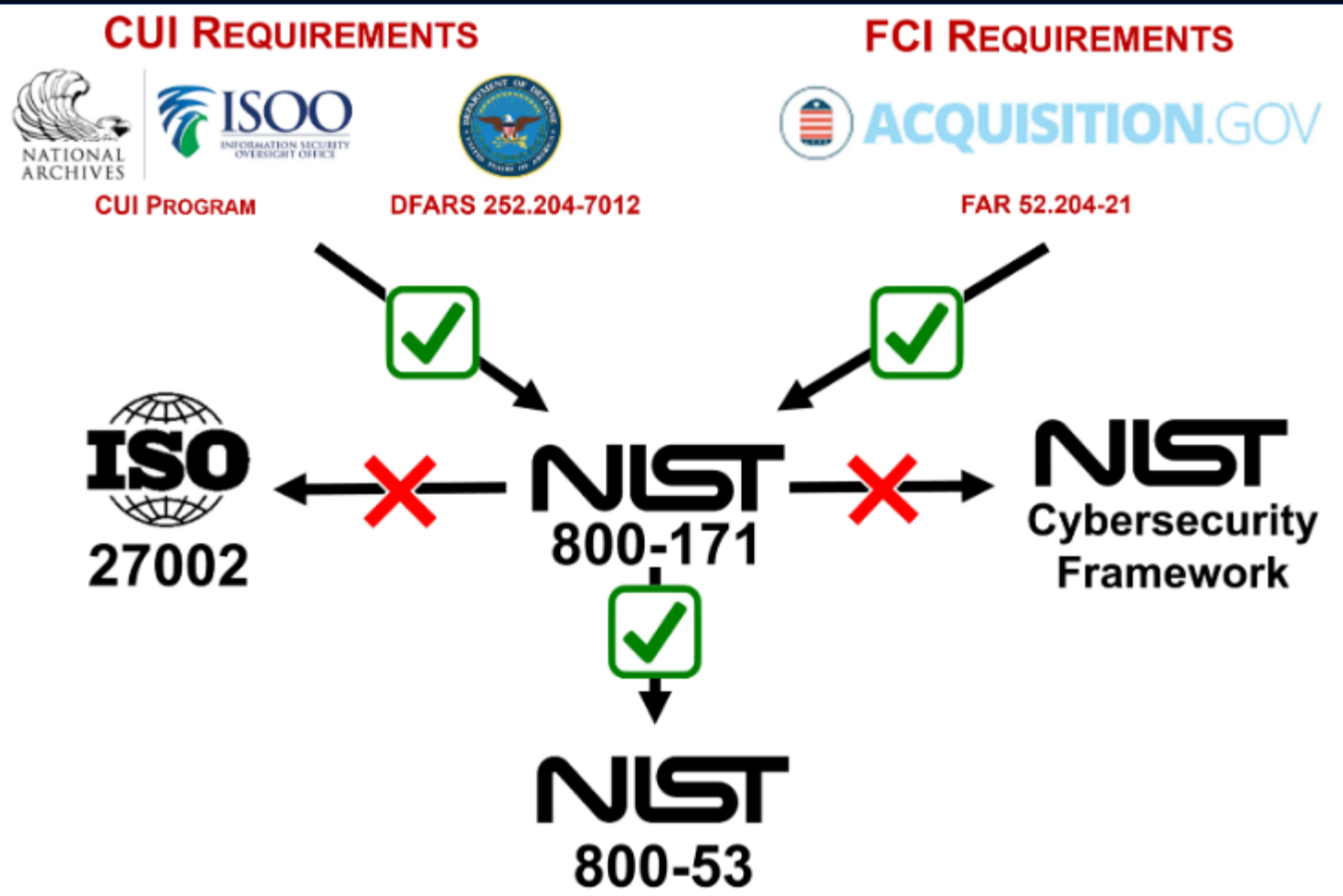
FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021

FAR 52.204-21, DFARS, NIST, and Beyond



An Evolution – Not a Departure

ACQUISITION.GOV

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

1. 15 Controls
2. Self-Attestation
3. Bare Minimum

What is FCI?

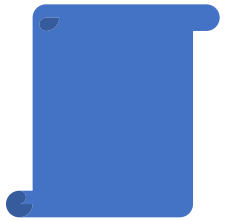
Federal contract information (from 48 CFR 52.204-21) means information, not intended for public release, that is **provided by or generated for the Government under a contract to develop or deliver a product or service to the Government**, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

FAR 52.204-21

The Contractor **shall** apply the following basic safeguarding requ irements and procedures to protect covered contractor information systems.

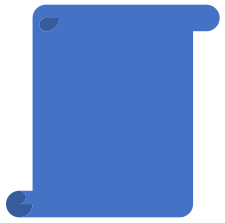
Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Key Points



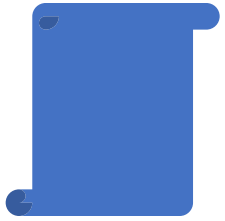
15 Controls

That cover “an inch deep but mile wide” through the information protection landscape.



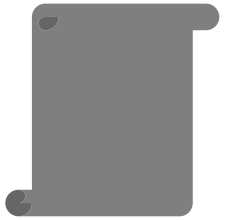
Are Echoed within NIST SP 800-171 Requirements

Complying with FAR 52.204-21 will always contribute to an attempt to comply with DFARS 252.204-7012



Considered Introductory

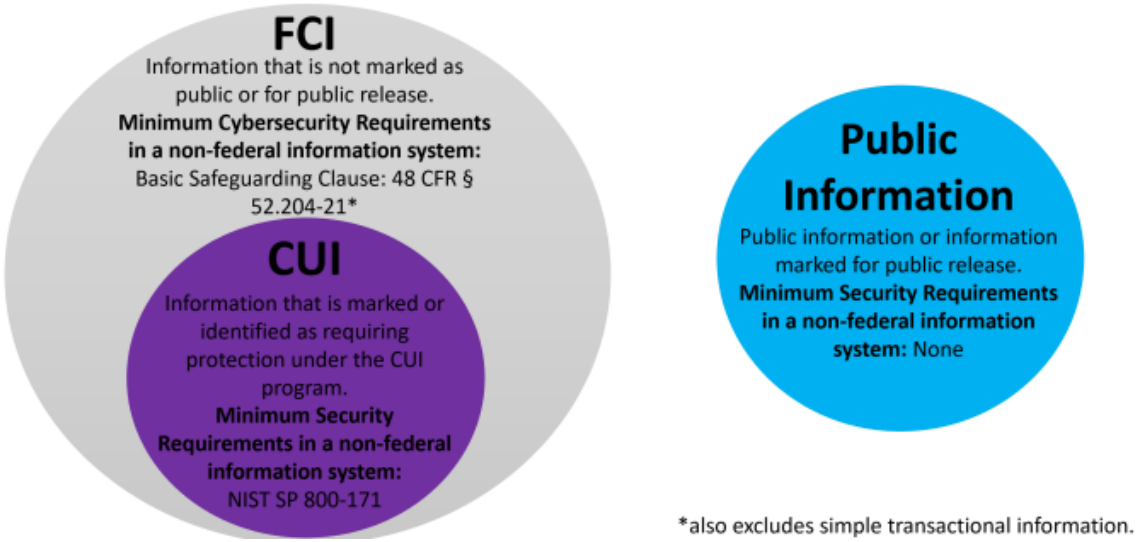
These controls represent minimal efforts, expense, and expertise to apply. “Common Sense” security.



They Are Maturing

CMMC Level 1 requirements will introduce a more formal approach to compliance with these controls.

Information that is collected, created, or received pursuant to a government contract



*also excludes simple transactional information.

1. Reports/Charts/Notes
2. Emails/Bills of Material
3. Contracts,
   Subcontracts,
   Purchase Orders

Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021

NATIONAL ARCHIVES

CONTROLLED UNCLASSIFIED INFORMATION

1

Definition

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls.

2

Categories

Archives.gov/cui/registry/category-list

3

Executive Agent

The National Archives and Records Administration.

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

NIST
National Institute of Standards and Technology

The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.

The Contractor shall notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement.

When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract… the Contractor shall rapidly report cyber incidents to DoD.

ACQUISITION.GOV

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

1. 14 Families
2. 110 Controls
3. Self-Attestation

14 Families – 110 Controls – 320 Audit Objectives

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification & Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

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.

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

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST Special Publication 800-18 Revision 1

1. NIST Special Publication 800-18
   Revision 1
   Guide for Developing Security Plans
   for Federal Information Systems

NIST SP 800-171r2

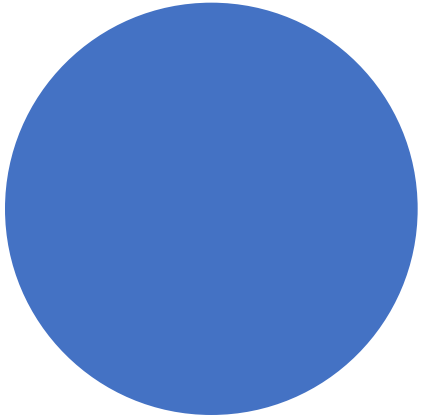
2. NIST Special Publication 800-171r2
   Protecting Controlled Unclassified
   Information in Nonfederal Systems
   and Organizations

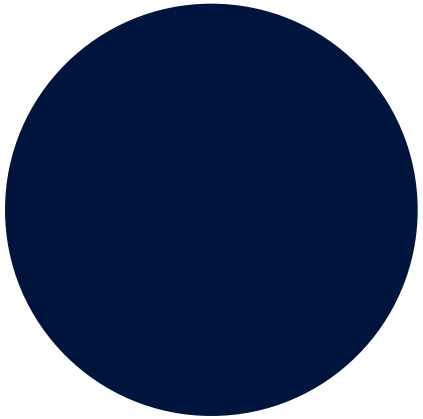
NIST SP 800-171A

3. NIST Special Publication 800-171A
   Assessing Security Requirements for
   Controlled Unclassified Information

Plan of Action and Milestones

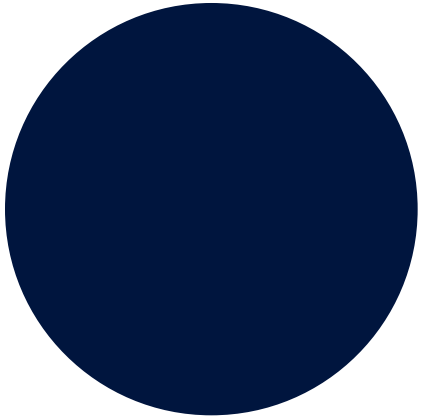
Tasks that need to be accomplished

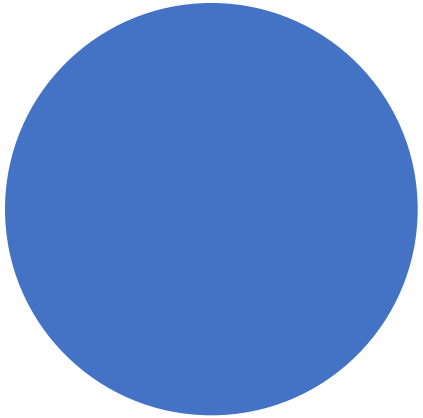




Milestones for meeting the tasks

Resources required to accomplish the elements of the plan





Scheduled completion dates for the milestones

Additional Internal Documents

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

Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

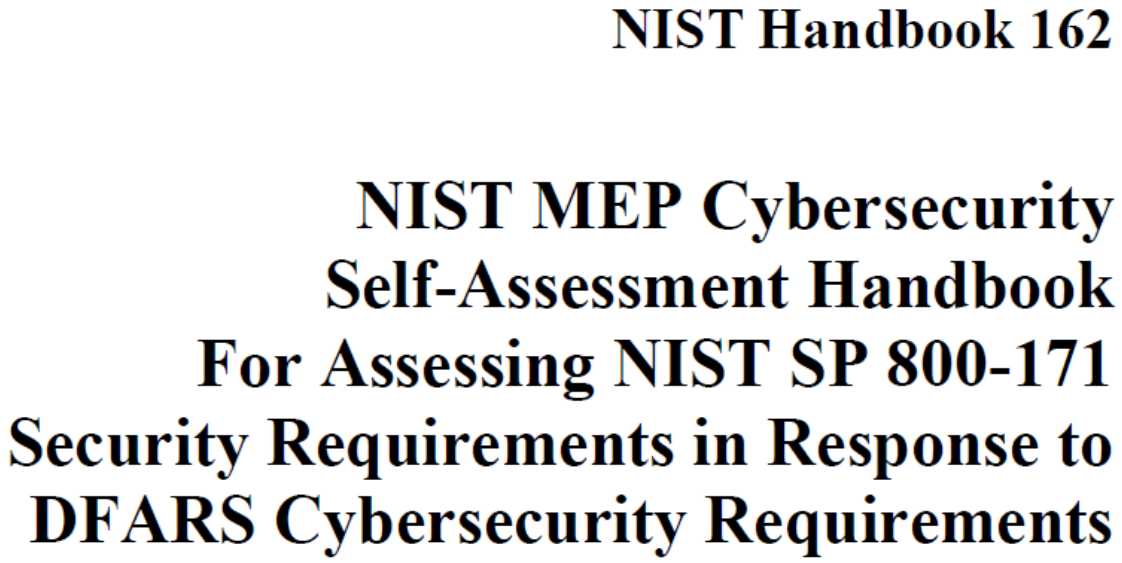
DFARS 252.204-7021

Why a Self-Assessment?

DFARS 252.204-7019

DFARS 252.204-7020

- ❑ Effects all contracts awarded on and after 30 NOV 2020.
- ❑ No existing minimum score requirements.
- ❑ Prime Contractor cannot access your score in SPRS – they must request from vendor directly.



1 NIST Handbook 162

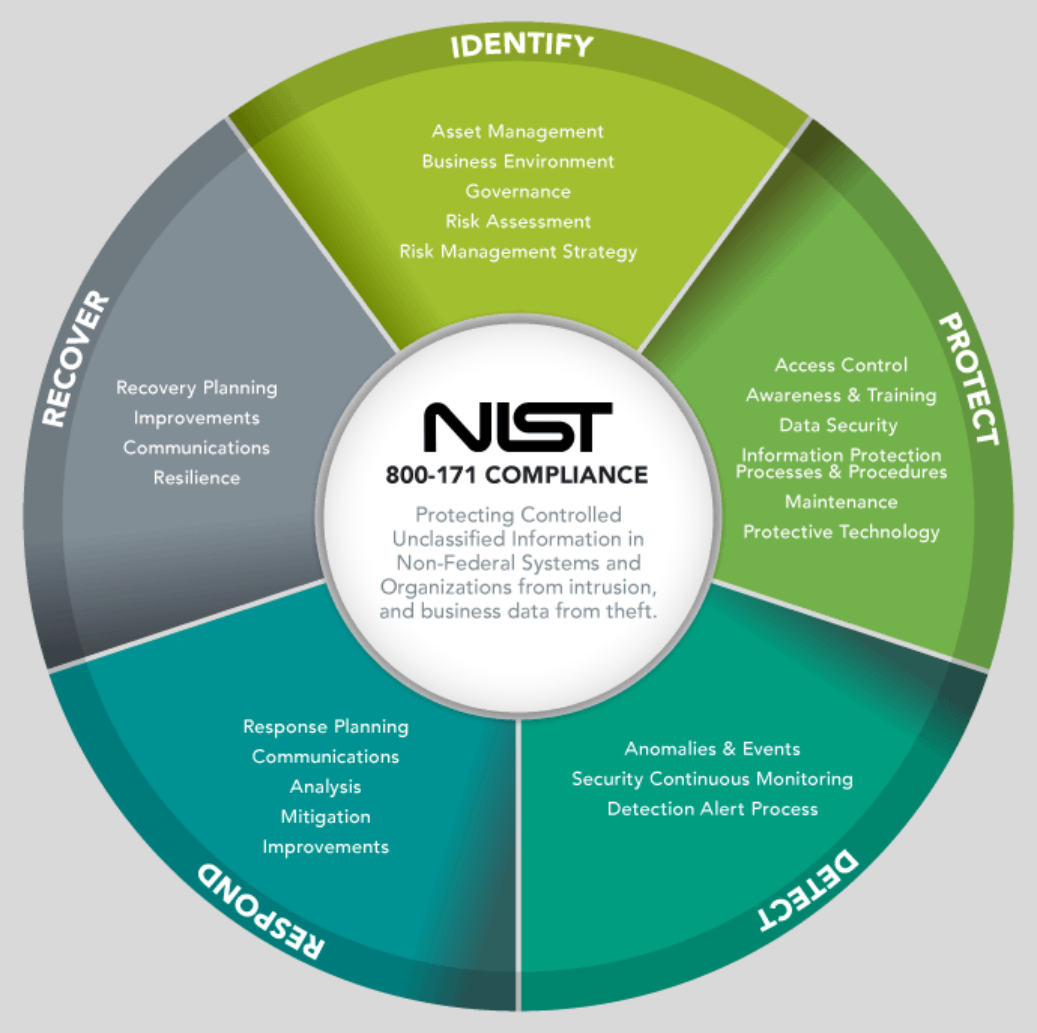
NIST MEP Cybersecurity Self-Assessment Handbook for Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

2 NIST SP 800-171A

NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information

3 DoD Memo

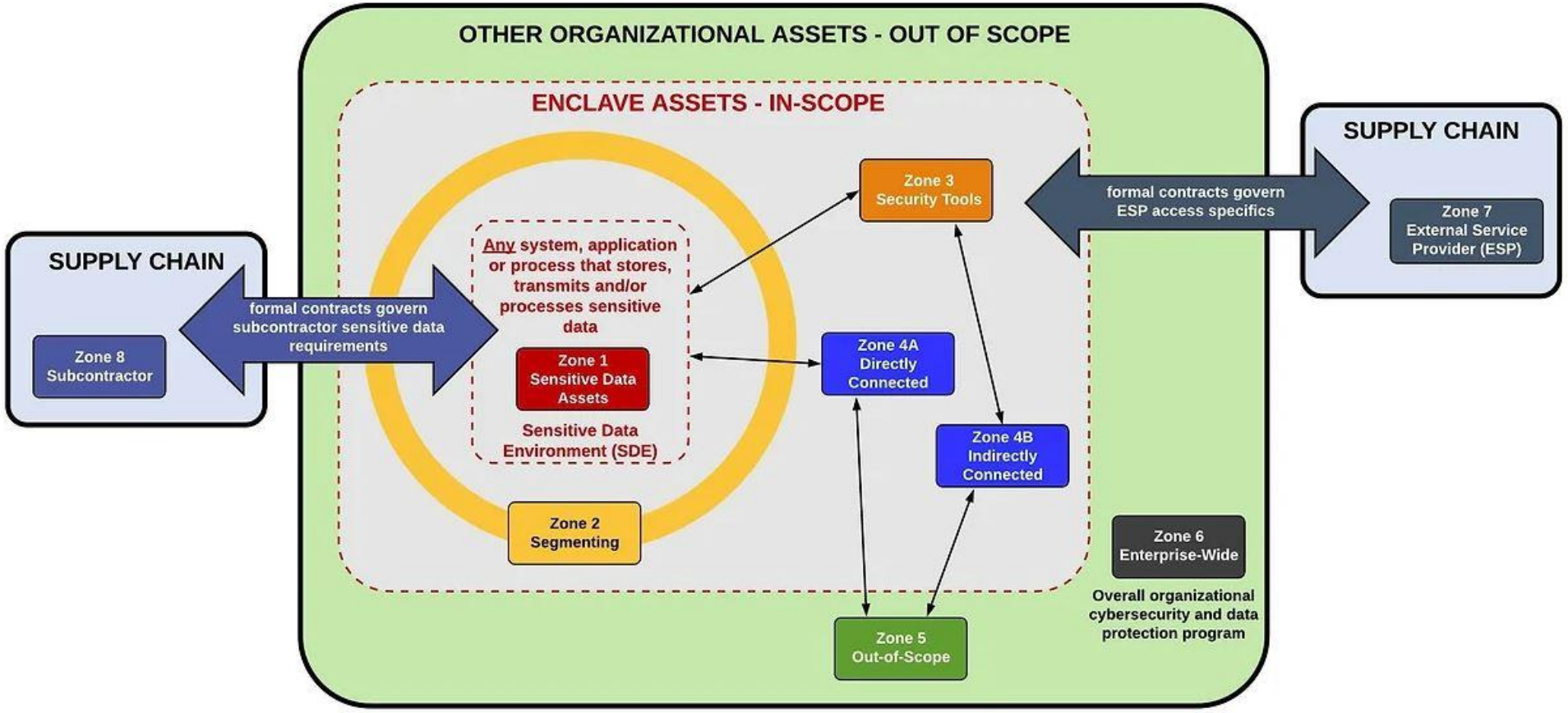
DoD Memo
DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements



NIST Basic Assessment and Score

- ❑ Conduct a NIST SP 800-171 Basic Assessment
- ❑ Post Summary Level Scores in the Supplier Performance Risk System (SPRS)
- ❑ Summary Level Scores cannot be older than 3 years

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

Assessment Process

ASSESSMENT Controls

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

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].

Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021

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
An APEX Accelerator

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).

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) 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.

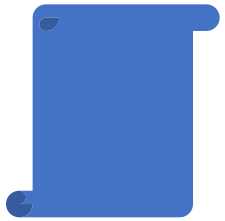
If the overall scoring of the Assessment after placing items on the Limited Practice Deficiency Correction program results in **greater than or equal to 80%** (88/110 practices “MET”), the OSC will be required to correct deficiencies.

Why the 48 CFR?

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

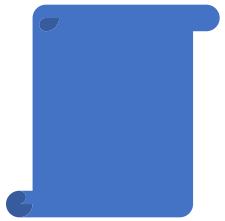
- 32 CFR defined the requirements. 48 CFR now makes it enforceable in actual contracts.

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



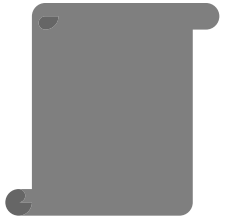
The New DFARS rule

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



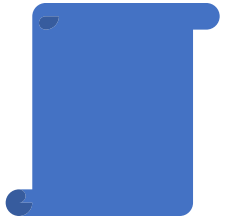
Contractual Clauses Added

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.

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.

Get Moving

CMMC will be a MANDATORY requirement.

This represents the transition from Self-Attestation to 3rd Party Validation.

- Map out a Plan
- Review your Documentation
- What about Your Suppliers?!

5
3

Agenda

01 The Federal Position on Zero Trust

02 FAR, DFARS, CMMC, and still more Acronyms

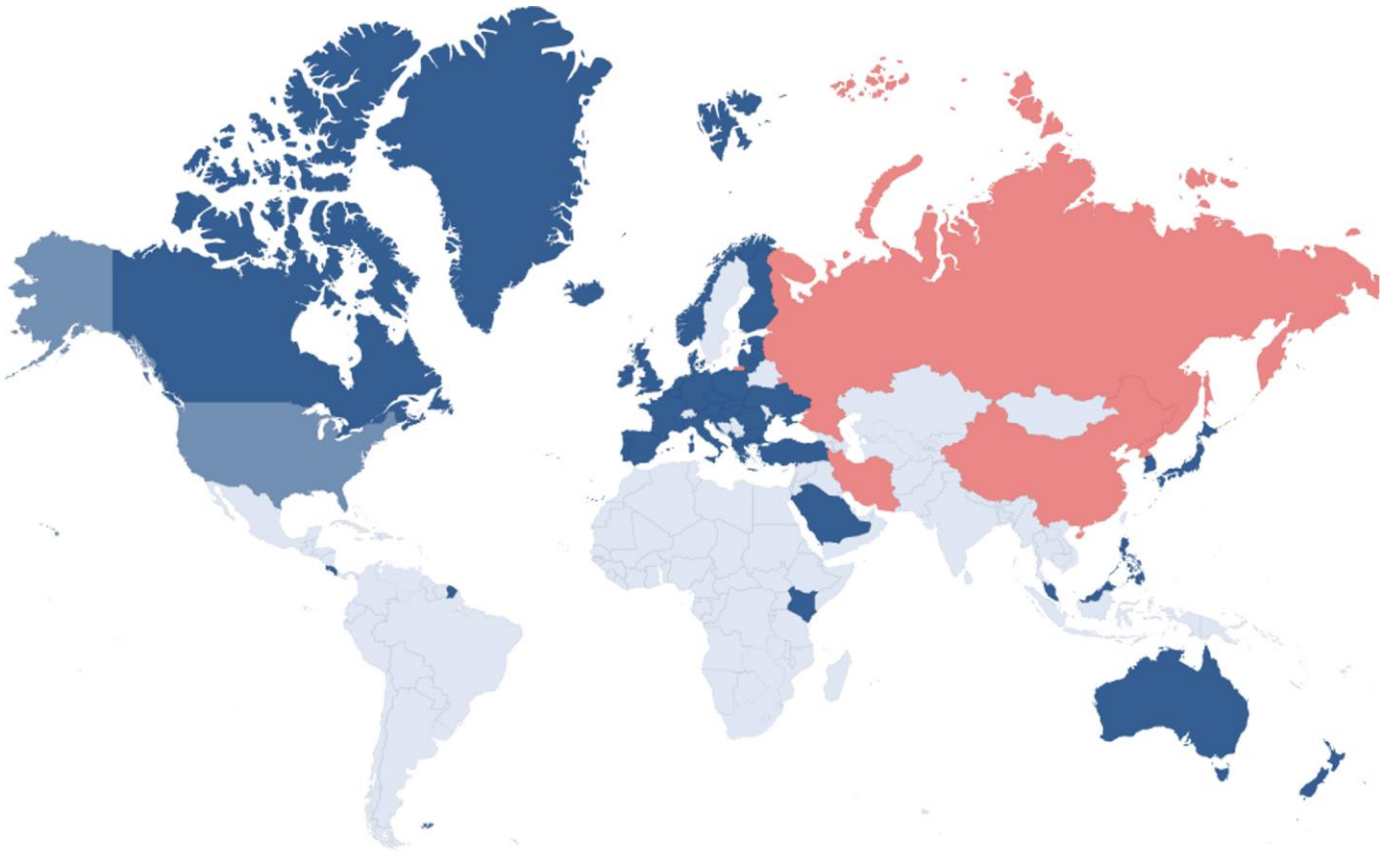
03 **Foreign Ownership, Control, or Influence (FOCI – yet another acronym)**

What is FOCI?

FOCI:

When a **foreign person or entity** is in a position of power, giving them access to classified or proprietary information and the ability to affect outcomes.

Gauge Your Risk

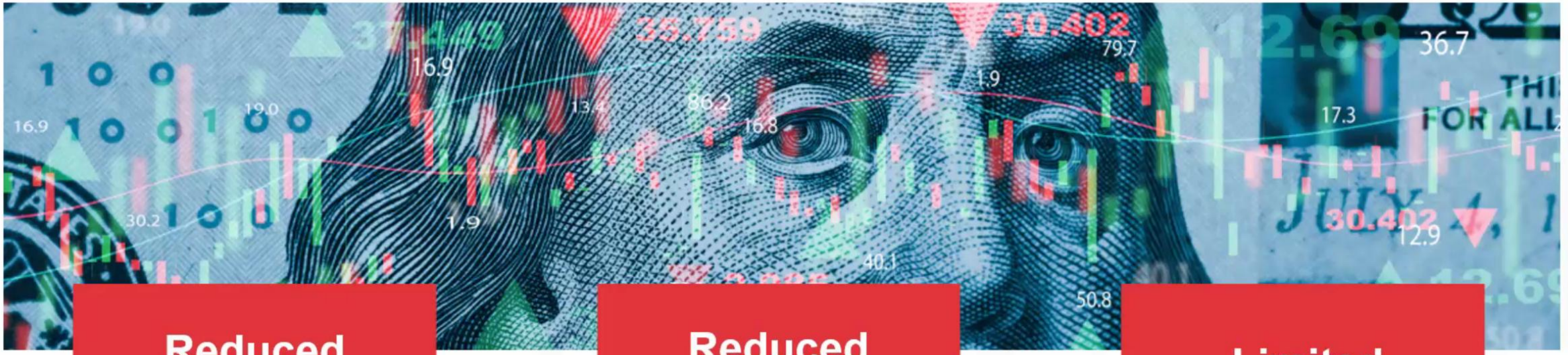


Close U.S. allies

Adversary or near-peer competitor nations

low SEVERITY OF RISK *high*

How can it affect you?



Reduced economic competitiveness

Reduced domestic investor interest

Limited government aid, awards, and contracts

Definitions

foreign:

foreign persons from a foreign country of concern

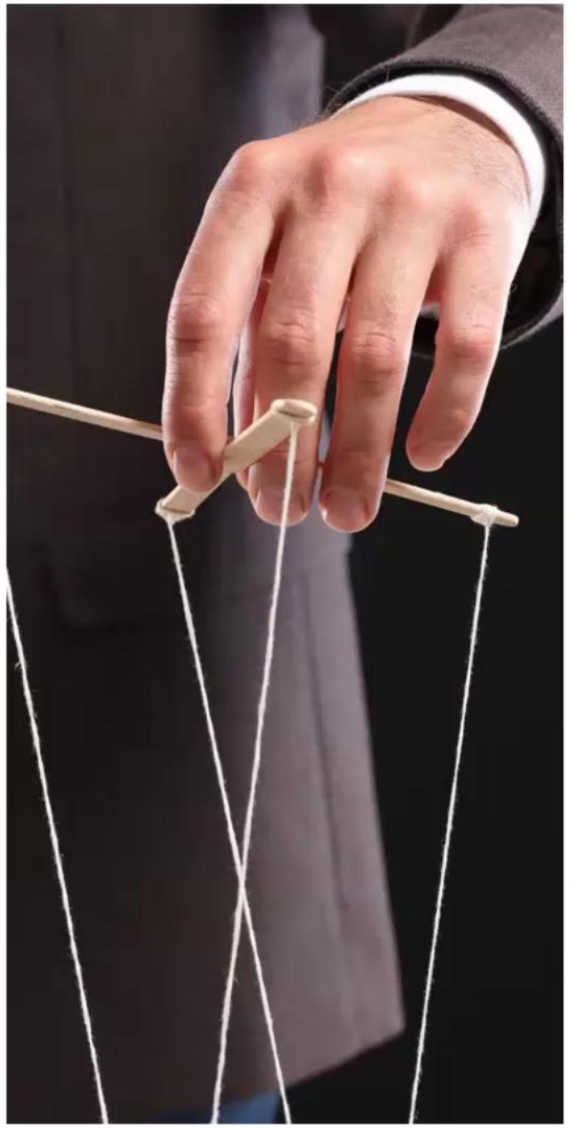
foreign person:

any entity controlled by a foreign national or entity

foreign country of concern:

China, North Korea, Russia, Iran

Definitions



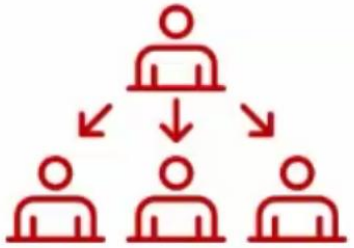
control:
foreign entity with power over business decisions

covered individual:
meaningful contributor to a project under a Federal research agency award

key management personnel:
entity officials with majority interest or decision-making authority

malign foreign talent recruitment program:
compensation for activities that may conflict with Federal award or contract

Types of Influence



Ability to direct or decide company matters

Position in foreign government

Debt liabilities or obligations

Supply chain located in a foreign country of concern

Contract between the company and foreign person or entity

Foreign government-connected customers

Collaborations with a foreign government-connected entity

REDUCING THE RISK OF FOCI PROTECTS FROM

unwanted technology transfer

negative impact on U.S. national security interests

loss of customers & revenue

loss of facility security clearance eligibility

loss of U.S. government assistance awards

CITATIONS

1. 15 U.S. Code § 638
2. 32 CFR § 2004.34
3. National Industrial Security Program Operating Manual (NISPOM), 32 CFR § 117.11(a)(1)
4. https://www.youtube.com/watch?v=GdapE82GceA
5. Public Law 117-183
6. NISPOM
7. Title 15 Subtitle B Chapter VII Subchapter C Part 740 Supplement No. 1
8. 17 CFR § 240.13d-3
9. NISPOM, 32 CFR § 117.11

VIDEO LINKS

Made In Beijing
http://y2u.be/GdapE82GceA

Inside the FBI Podcast: The China Threat
http://y2u.be/-vE6dDBPOaQ

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.

- ~~**November 5** – Certification Programs for Women and Veteran Owned Businesses~~
- ~~**November 12** – Getting Started w DLA/DIBBS for Contractor & Subcontractors Part 1~~
- ~~**November 19** – Getting Started w DLA/DIBBS for Contractor & Subcontractors Part 2~~
- **December 3** – DCMA Overview
- **December 17** – Understanding the US SBA and DOD Mentor Protégé Programs (MPP)

…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

November 20 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

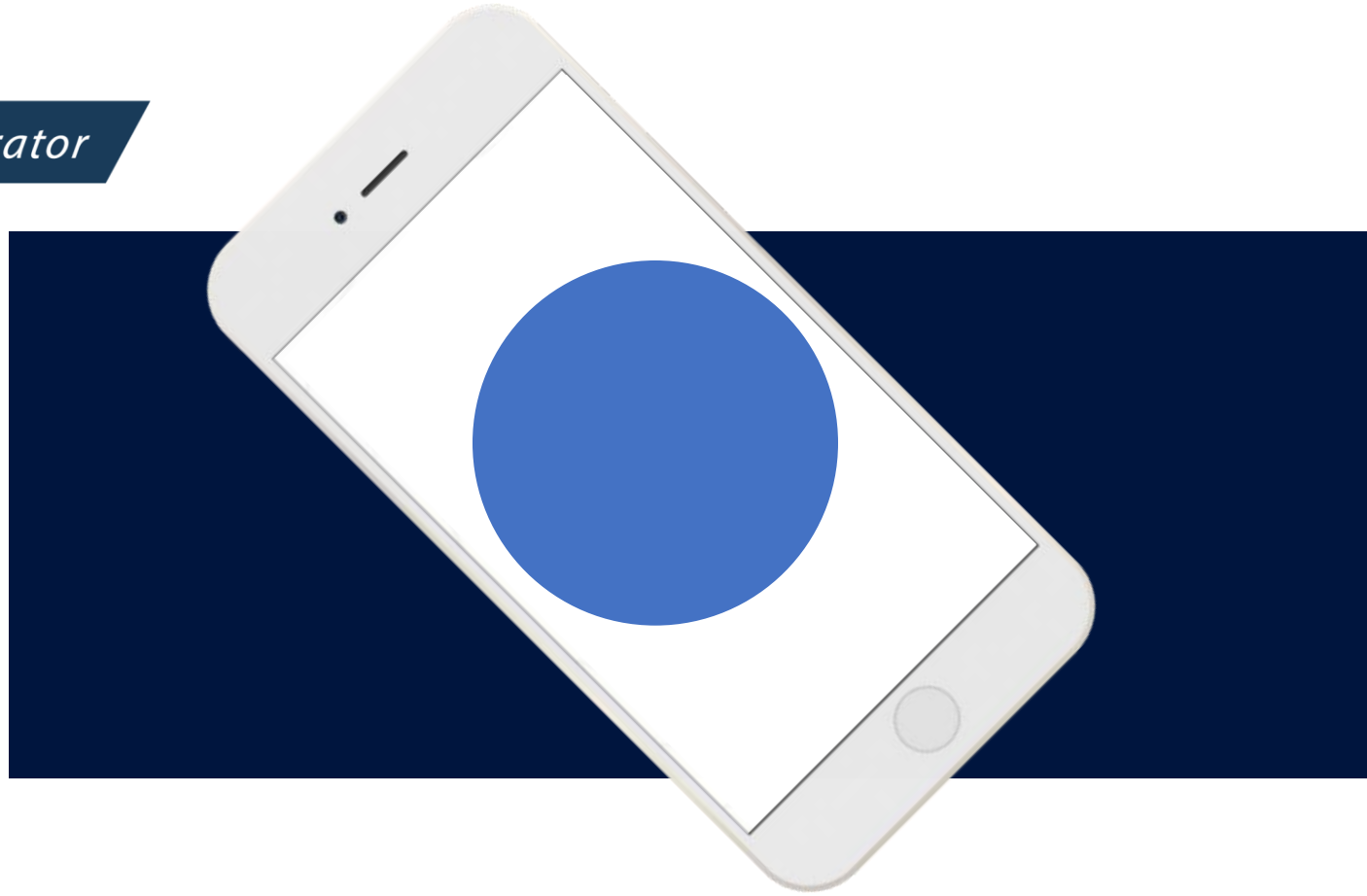
10437 Innovation Drive Suite 320
Milwaukee WI 53226

Wisconsin Procurement Institute

An APEX Accelerator

Matthew Frost

mattf@wispro.org



APEX ACCELERATORS