



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**

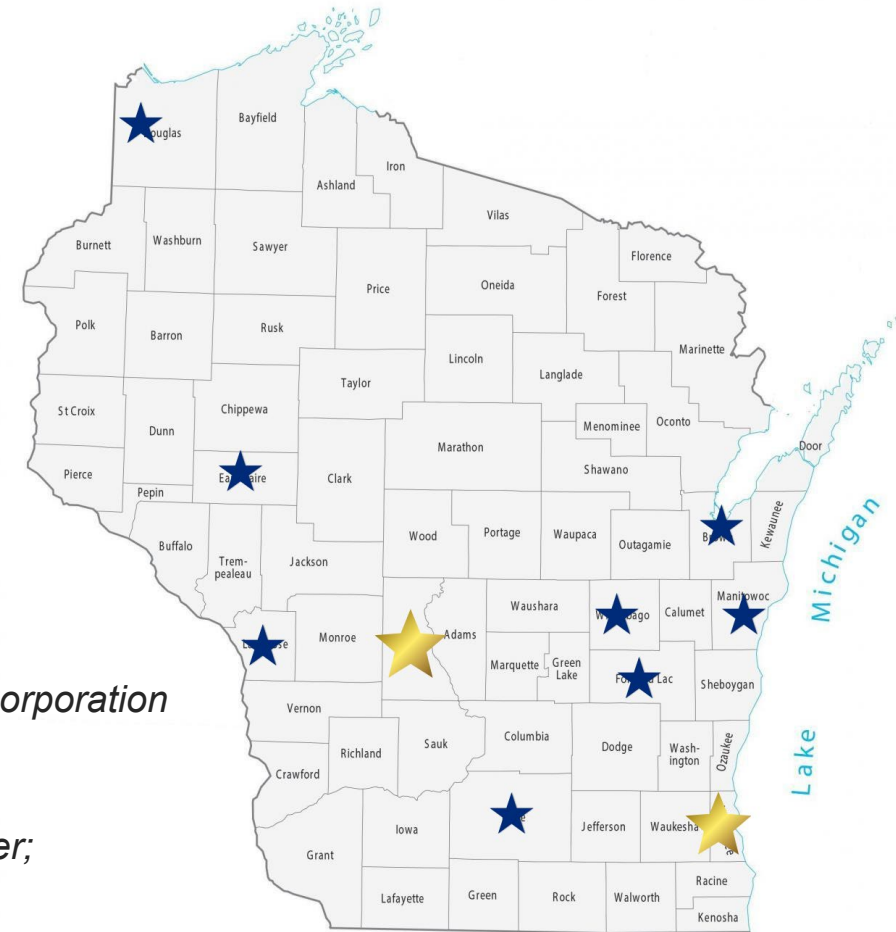
- *Progress Lakeshore*

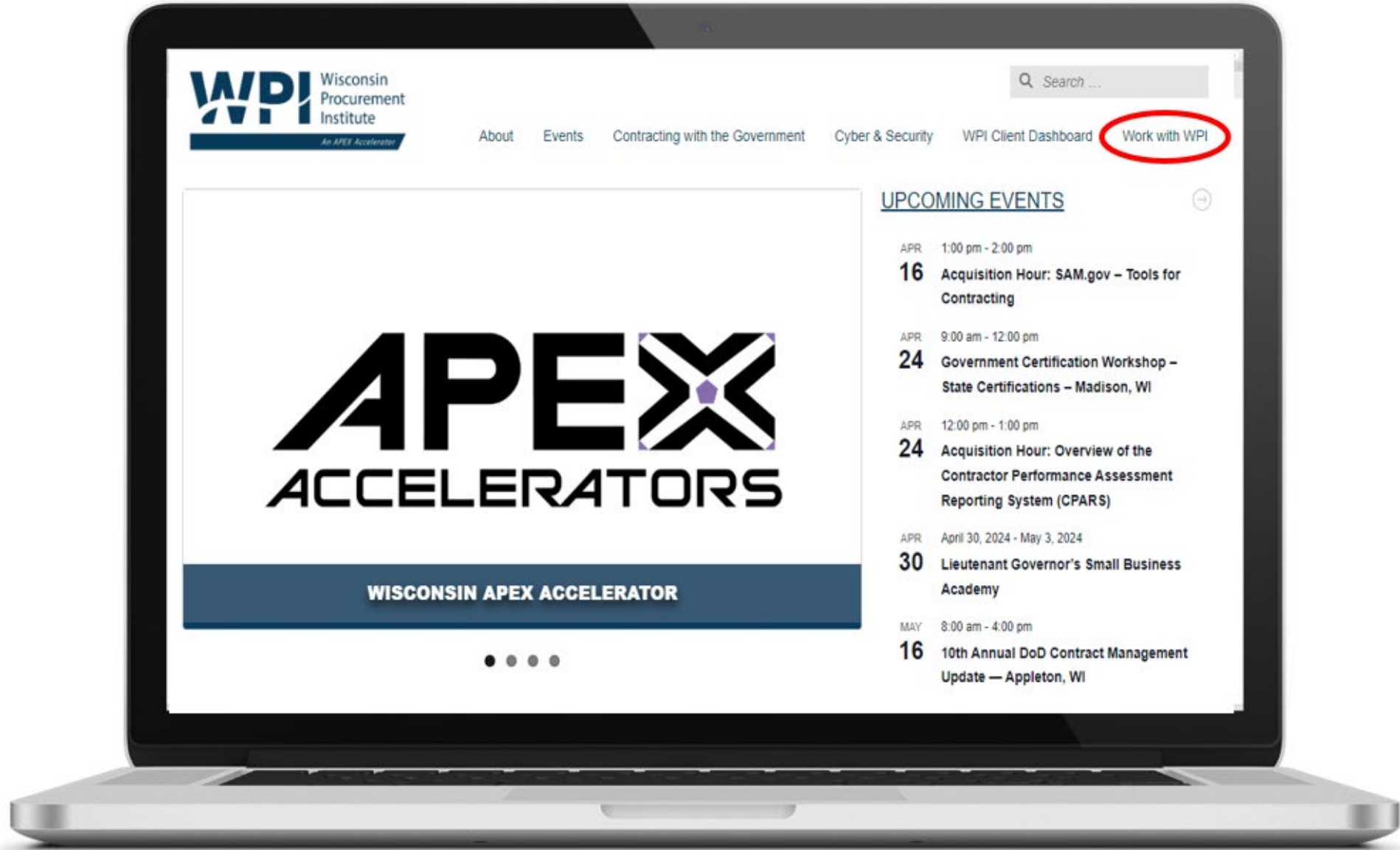
- **OSHKOSH**

- *Greater Oshkosh Economic Development Corporation*

- **SUPERIOR**

- *Small Business Dev Center; UW Superior*







Wisconsin
Procurement
Institute

An APEX Accelerator

DMSCC: The CMMC Timeline



October 21st, 2025

Agenda

01

Past:
What is CMMC and where does it come from?
CMMC's evolution, the intentions of change and certification.

02

Present:
The CMMC Program as defined by 32 CFR and current state of assessment environment.

03

Future:
Enforcement in solicitations, 48 CFR, and beyond.





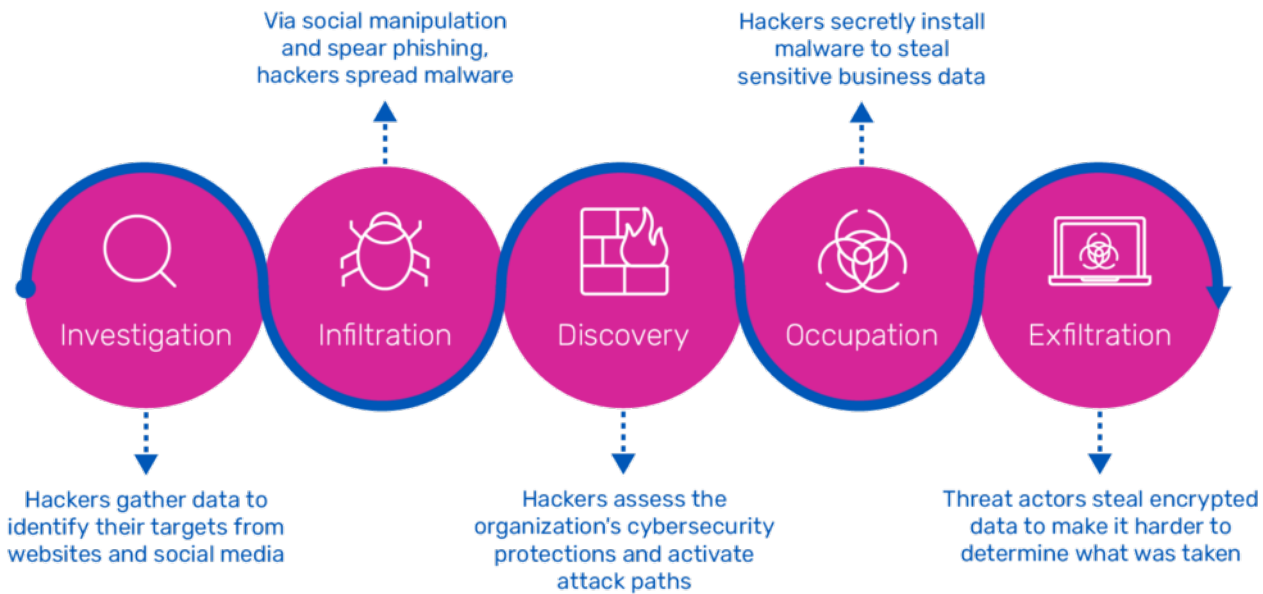
Confirmed in 2013, the theft of data from the F-35 Lightning II represented one of the most significant data breaches in world history.

Breach involved a series of units, funded and operated by the PLA, identified as Advanced Persistent Threats (APT).

Targets were companies within Lockheed Martin's supply chain.

Data was primarily unclassified, but controlled, information.

What is an Advanced Persistent Threat?







Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021



52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

1

15 Controls

2

Self-Attestation

3

CMMC Level 1

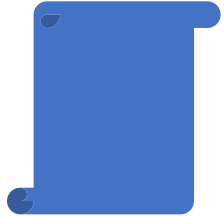
What is FCI?

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.

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

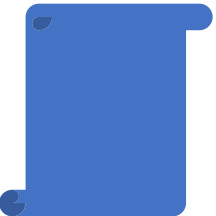
Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Key Points



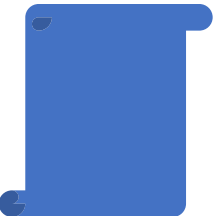
15 Controls

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



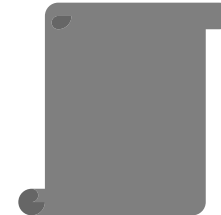
Are Echoed within NIST SP 800-171 Requirements

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



Considered Introductory

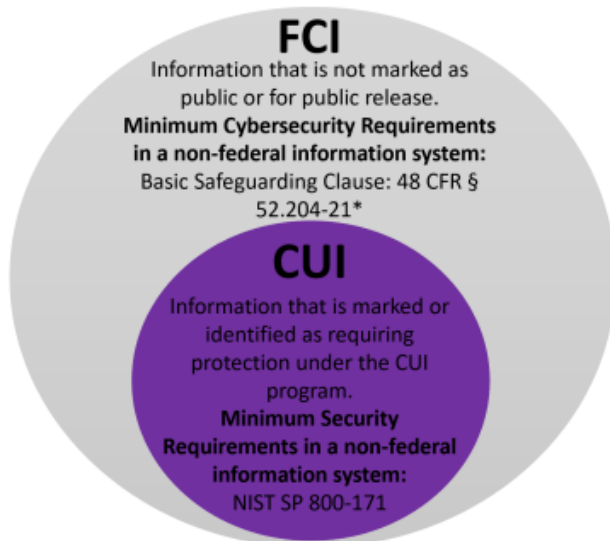
These controls represent minimal efforts, expense, and expertise to apply. “Common Sense” security.



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

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.



**252.204-7012 Safeguarding
Covered Defense Information
and Cyber Incident Reporting**

1

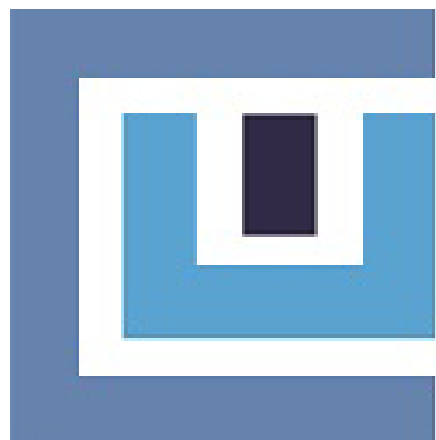
14 Families

2

110 Controls

3

Self-Attestation



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](https://www.archives.gov/cui/registry/category-list)

3

Executive Agent

The National Archives and Records Administration.

NIST SP 800-171r2 Reporting Requirements

Chapter 3: Page 9 NIST SP 800-171r2

(c) *Cyber incident reporting requirement.*

(1) 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 that are designated as operationally critical support and identified in the contract, the Contractor shall—

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at <https://dibnet.dod.mil>.

(2) *Cyber incident report.* The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at <https://dibnet.dod.mil>.

(3) *Medium assurance certificate requirement.* In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see <https://public.cyber.mil/eca/>.

(d) *Malicious software.* When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) *Media preservation and protection.* When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) *Access to additional information or equipment necessary for forensic analysis.* Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) *Cyber incident damage assessment activities.* If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.



Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021

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

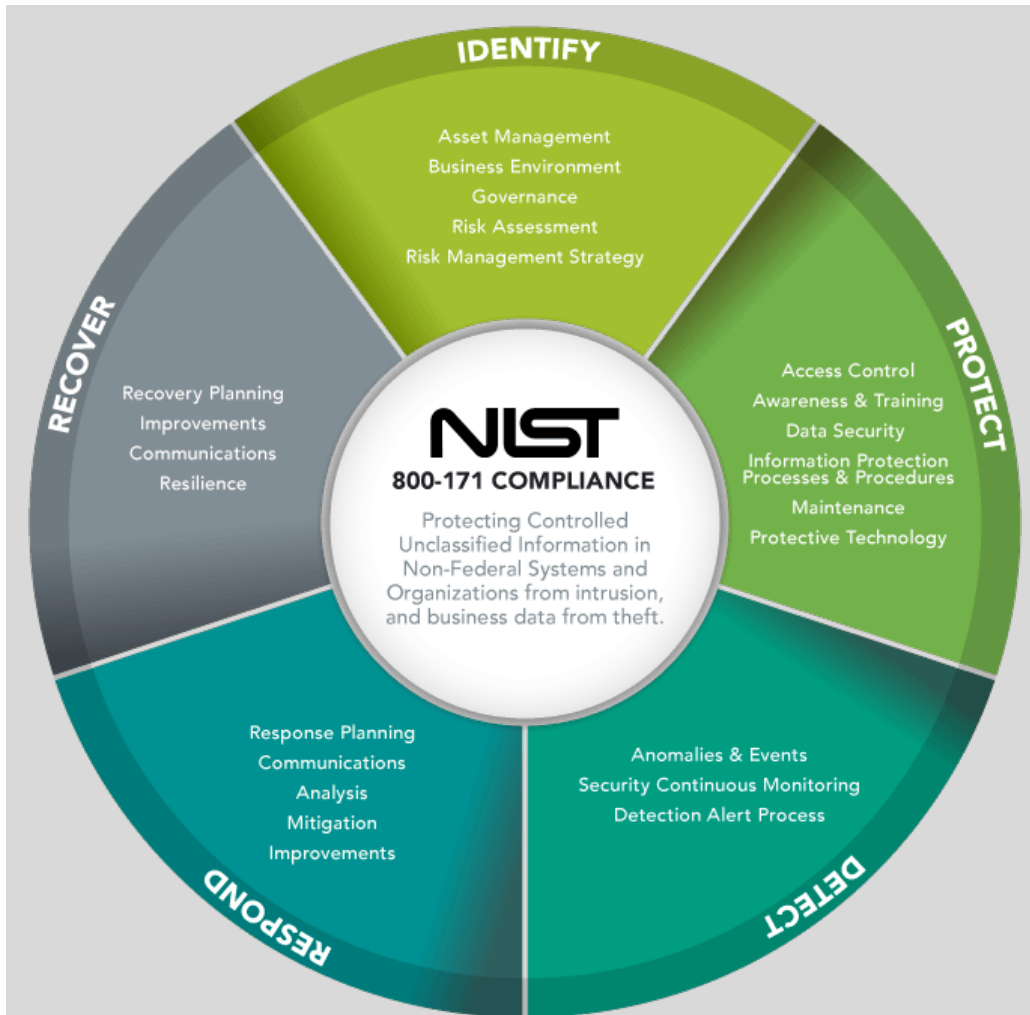
NIST SP 800-171A

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



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

Why a Self-Assessment?

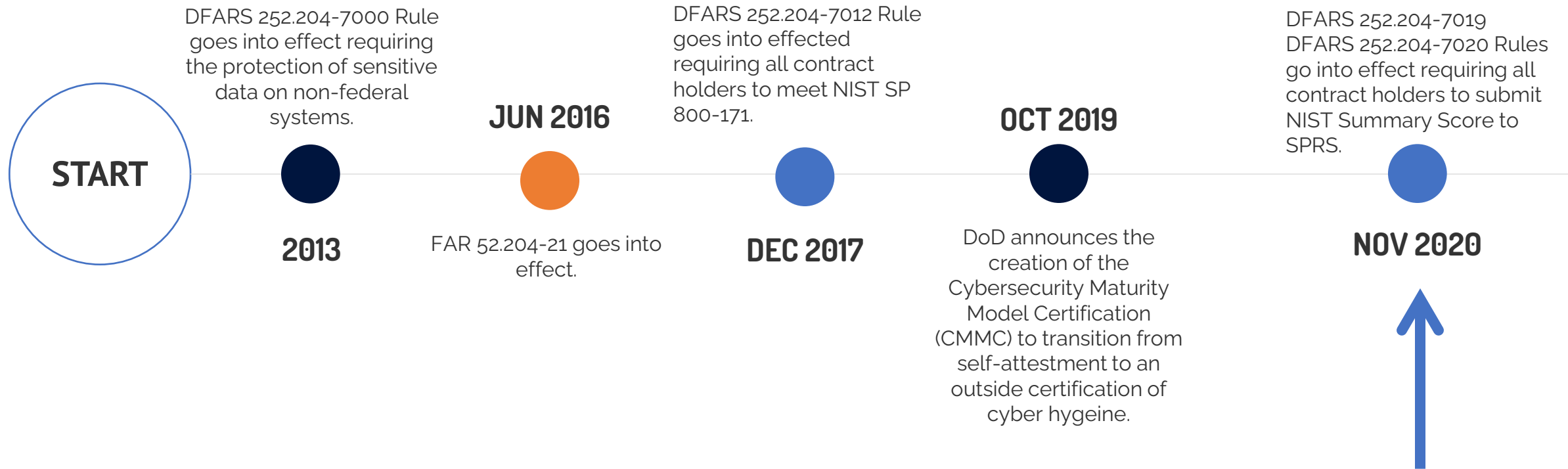
DFARS 252.204-7019

DFARS 252.204-7020

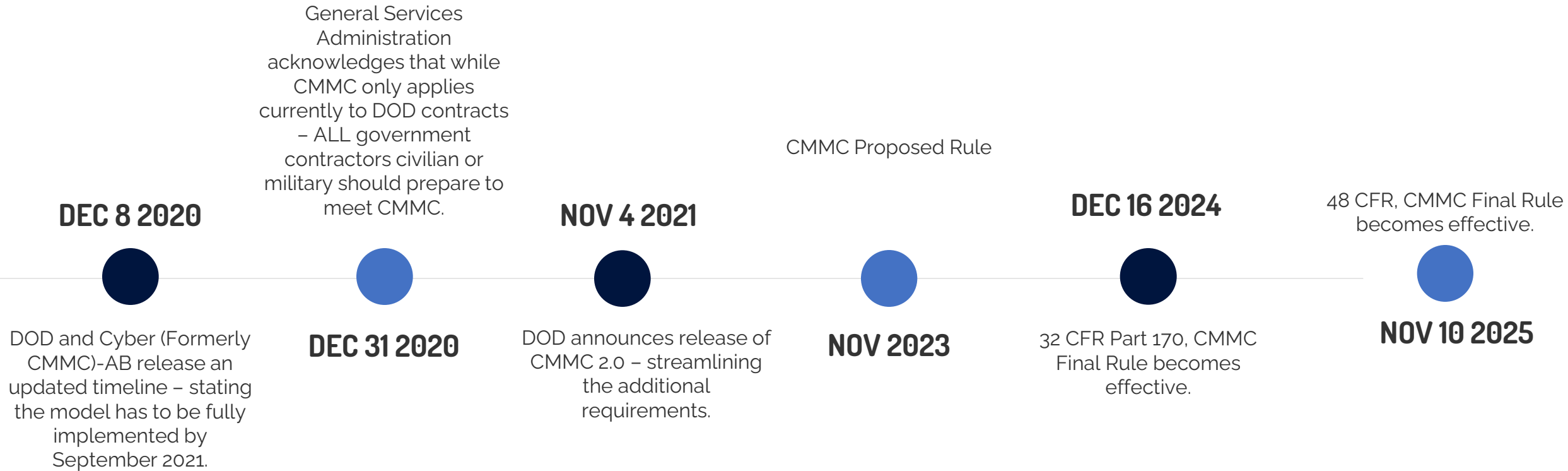
- ❑ Effects all contracts awarded on and after 30 NOV 2020.
- ❑ No existing minimum score requirements.
- ❑ Prime Contractor cannot access your score in SPRS – they must request from vendor directly.



Cybersecurity Timeline



Cybersecurity Timeline



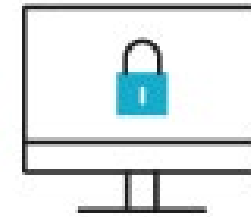
What is CMMC?



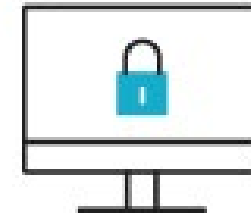
Department of Defense
certification process that...



measures the ability
of members of the
Defense industrial
base (DIB) to
protect...



Federal Contract
Information (FCI)



Controlled
Unclassified
Information (CUI)

The Cybersecurity Maturity Model Certification (CMMC) is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices...



(b) Requirements. The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

Agenda

01

Past:
What is CMMC and where does it come from? CMMC's evolution, the intentions of change and certification.

02

Present:
The CMMC Program as defined by 32 CFR and current state of assessment environment.

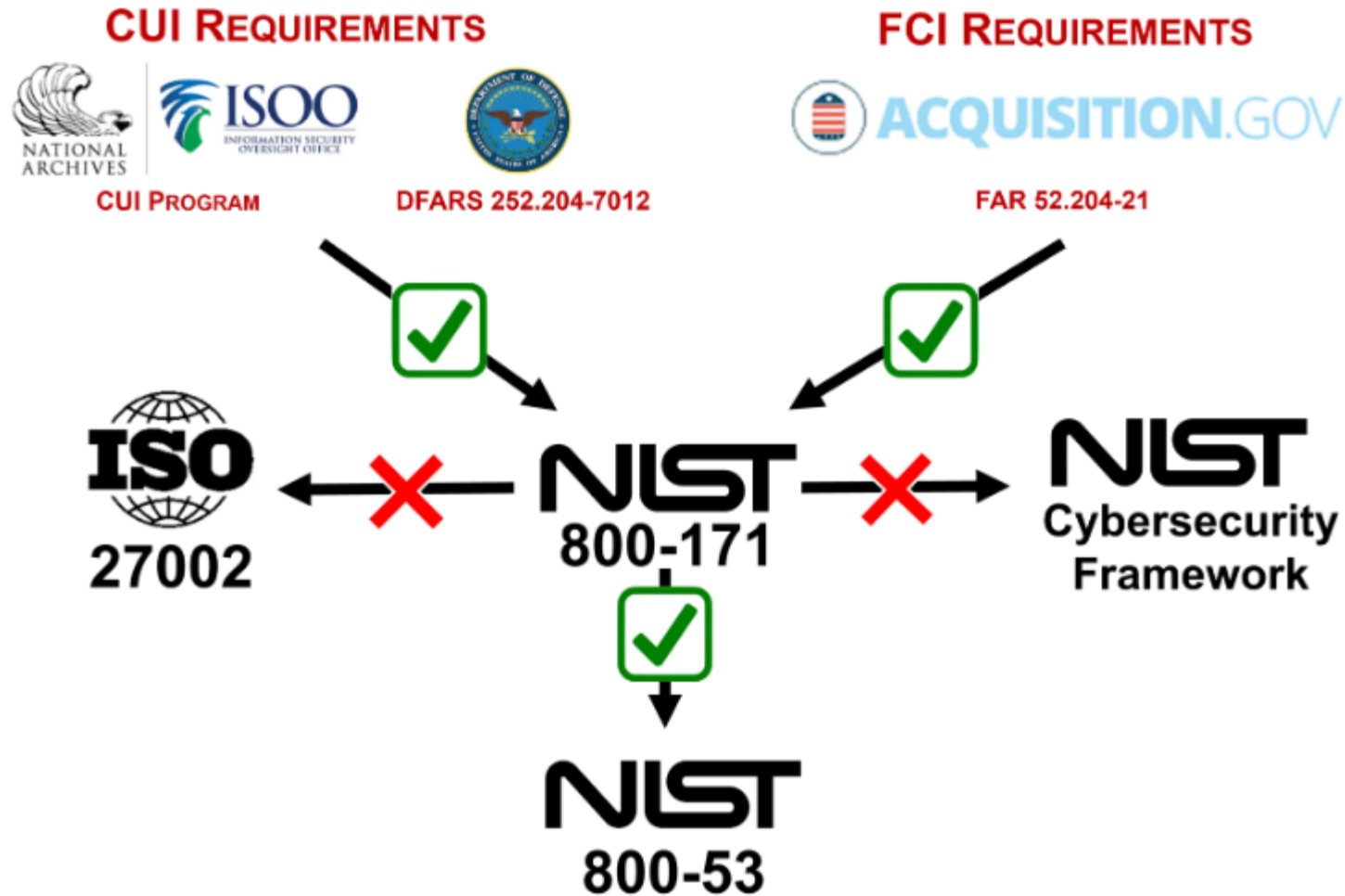
03

Future:
Enforcement in solicitations, 48 CFR, and beyond.

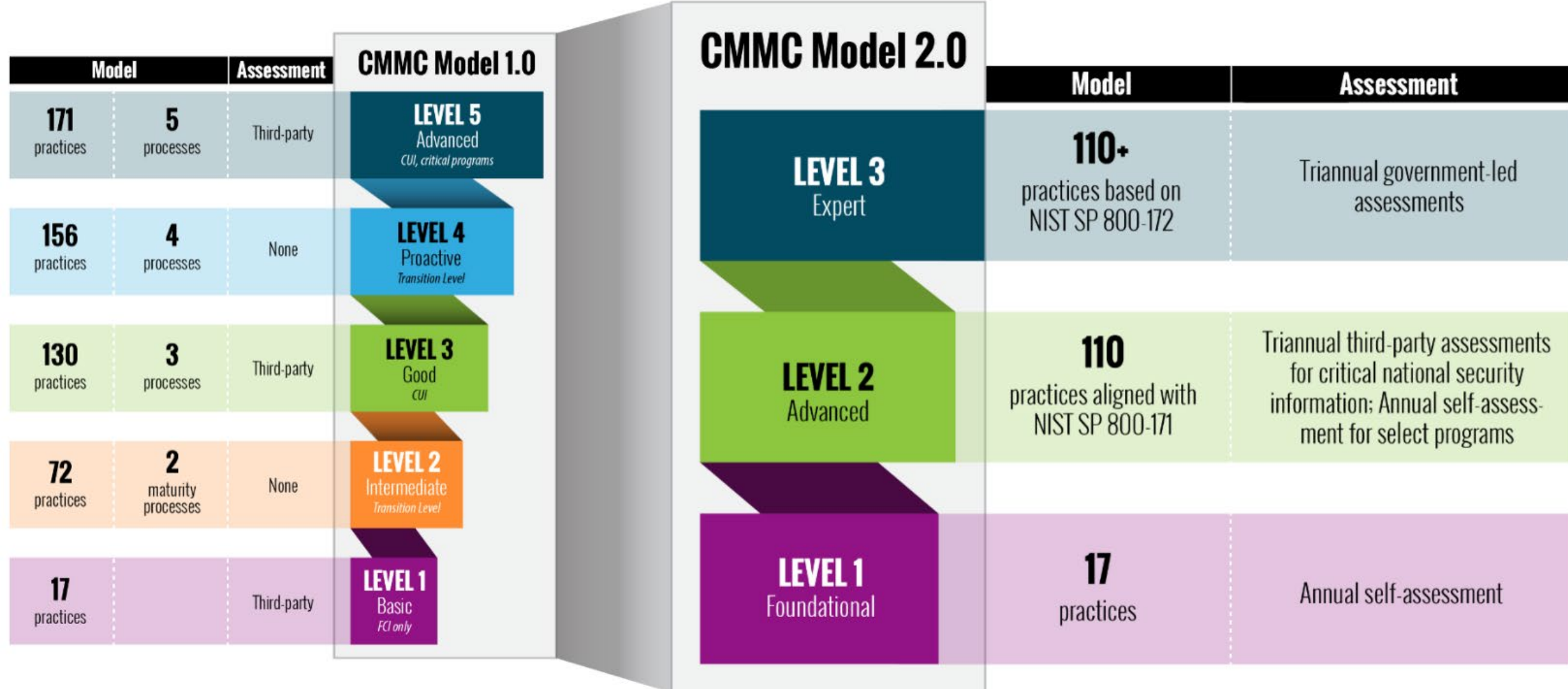


The CMMC Final Rule was published on **October 15, 2024**. It **BECAME** effective on **Dec 16, 2024**, and can now enter contracts and solicitations.

FAR 52.204-21, DFARS, NIST and CMMC



An Evolution – Not a Departure



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) ...	<ul style="list-style-type: none"> 15 required by FAR clause 52.204–21. 	<ul style="list-style-type: none"> Conducted by Organization Seeking Assessment (OSA) annually. Results entered into SPRS (or its successor capability). 	<ul style="list-style-type: none"> Not permitted 	<ul style="list-style-type: none"> After each assessment. Entered into SPRS.
Level 2 (Self) ...	<ul style="list-style-type: none"> 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> After each assessment and annually thereafter. Assessment will lapse upon failure to annually affirm. Entered into SPRS (or its successor capability).
Level 2 (C3PAO).	<ul style="list-style-type: none"> 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> After each assessment and annually thereafter. Assessment will lapse upon failure to annually affirm. Entered into SPRS (or its successor capability).
Level 3 (DIBCAC).	<ul style="list-style-type: none"> 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). 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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



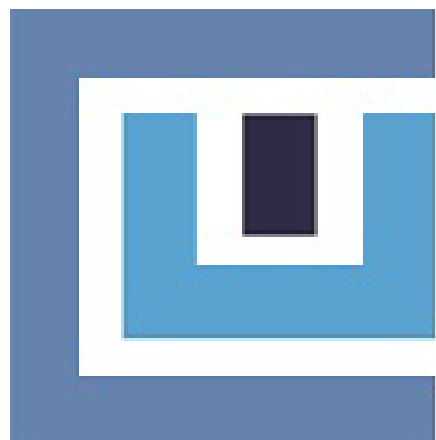
The Contractor **shall** apply the following basic safeguarding requirements and procedures to protect covered contractor information systems.

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

Supplier Performance Risk System

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





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](https://www.archives.gov/cui/registry/category-list)

3

Executive Agent

The National Archives and Records Administration.

SCOPING THE ASSESSMENT



INFORMATION

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

SECURITY ASSETS

- Digital Hardware
- Software
- Cloud Services

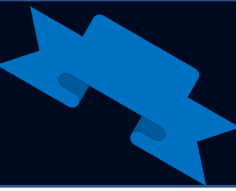
PRINTED MATERIAL

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

PERSONNEL

- U.S Persons
- Principle of Least Privilege

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**.



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.

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

Supplier Performance Risk System

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



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.



ABOUT US ▼

ACCREDITATION ▼

RESOURCES ▼

CMMC ECOSYSTEM ▼

NEWS & EVENTS ▼

MARKETPLACE

CAICO

www.cyberab.org

CMMC Assessment



Pre-Assessment:

- Hire a C3PAO
- Provide SSP and Supporting Documentation
- Schedule Assessment

Assessment:

Interview
Examine
Test

Post Assessment:

Submits report to Cyber-AB.
CMMC-AB performs quality check.
CMMC-AB issues report that confirms certification..
May allow limited use of POAM.

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.

Agenda

01

Past:
What is CMMC and where does it come from? CMMC's evolution, the intentions of change and certification.

02

Present:
The CMMC Program as defined by 32 CFR and current state of assessment environment.

03

Future:
Enforcement in solicitations, 48 CFR, and beyond.





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)

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

252.204-7021 Cybersecurity Maturity Model Certification Requirements.

As prescribed in 204.7503(a) and (b), insert the following clause:

CYBERSECURITY MATURITY MODEL CERTIFICATION REQUIREMENTS (JAN 2023)

(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see <https://www.acq.osd.mil/cmmc/index.html>).

(b) *Requirements.* The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts.* The Contractor shall—

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial products or commercial services, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

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) ...	<ul style="list-style-type: none"> 15 required by FAR clause 52.204–21. 	<ul style="list-style-type: none"> Conducted by Organization Seeking Assessment (OSA) annually. Results entered into SPRS (or its successor capability). 	<ul style="list-style-type: none"> Not permitted 	<ul style="list-style-type: none"> After each assessment. Entered into SPRS.
Level 2 (Self) ...	<ul style="list-style-type: none"> 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> After each assessment and annually thereafter. Assessment will lapse upon failure to annually affirm. Entered into SPRS (or its successor capability).
Level 2 (C3PAO).	<ul style="list-style-type: none"> 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> After each assessment and annually thereafter. Assessment will lapse upon failure to annually affirm. Entered into SPRS (or its successor capability).
Level 3 (DIBCAC).	<ul style="list-style-type: none"> 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). 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> 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 (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.

48 CFR and Beyond

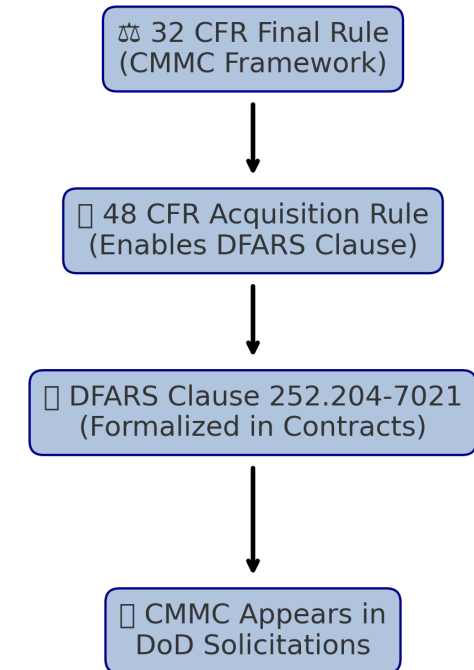
What is the 48 CFR?

- 48 Code of Federal Regulations
- Governs DoD acquisition regulations
- Enables DFARS clause 252.204-7021
- Adds CMMC Requirements to Solicitations

Current Status?

- Submitted to OIRA (Office of Information and Regulatory Affairs)
- Expected to be Finalized by end of Q3
- Believed to have a 365 day implementation window

How the 48 CFR Rule Enables CMMC Enforcement





[ABOUT US](#) ▼

[ACCREDITATION](#) ▼

[RESOURCES](#) ▼

[CMMC ECOSYSTEM](#) ▼

[NEWS & EVENTS](#) ▼

[MARKETPLACE](#)

[CAICO](#)

www.cyberab.org

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.

Upcoming Events

February 7, 2025

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.

- **October 22**– Federal Acquisition Regulations (FAR) Overview
- **November 5**– Certification Programs for Women and Veteran Owned Businesses
- **November 12**– Getting Started with DLA/DIBBS for Contractor and Subcontractors Part 1
- **November 19**– Getting Started with DLA/DIBBS for Contractor and Subcontractors Part 2
- **December 3**– DCMA Overview

...More information and registrations at wispro.org/events

CYBER THURSDAYS

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.

- **October 30**– CMMC and ITAR – Navigating the Differences and Where They Overlap
- **November 20**– Federal Cyber Update – A Review of Current Regulations
- **December 18**– CMMC From Top to Bottom – A Program Review

...More information and registrations at wispro.org/events

Upcoming Events



**The
Contracting
Academy**

*Developing and Growing
Government Contractors*

Dec 9

The Contracting Academy (TCA)

Virtual

...More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | CyberNewsletter
Events Newsletter

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

mattf@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226