Cyber Friday:

CMMC: Maintaining Your CMMC Certification

May 30 | 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute

WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

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.

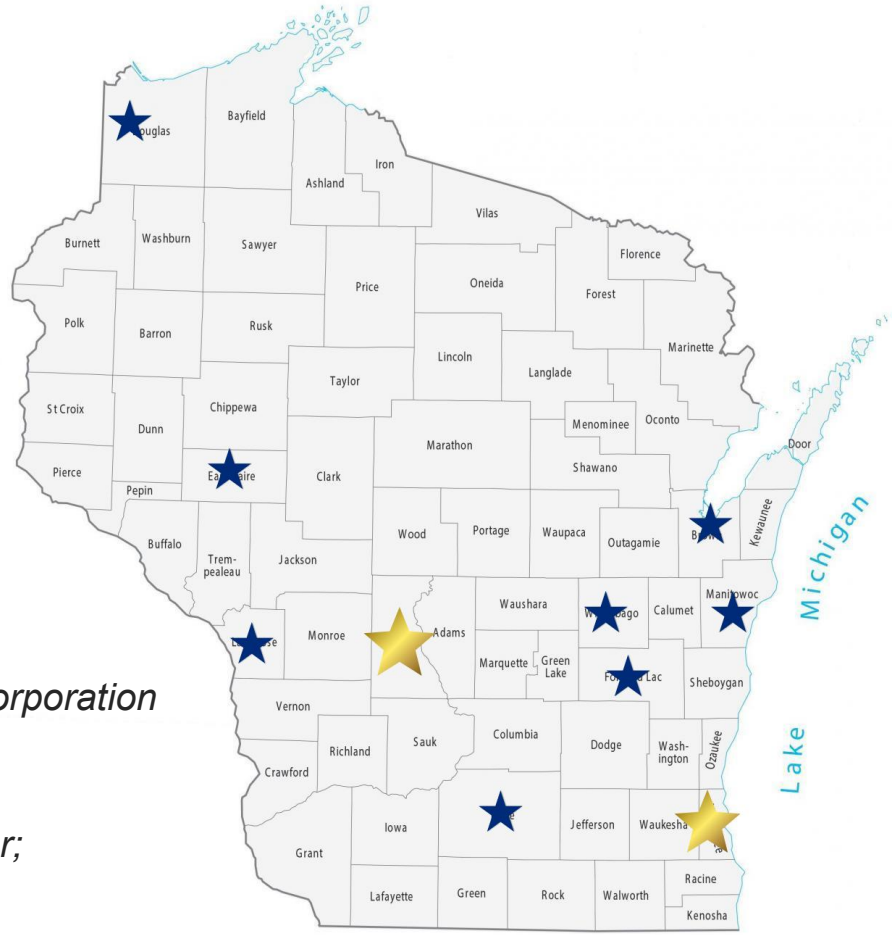
WPI provides services and training to all of Wisconsin's 72 counties

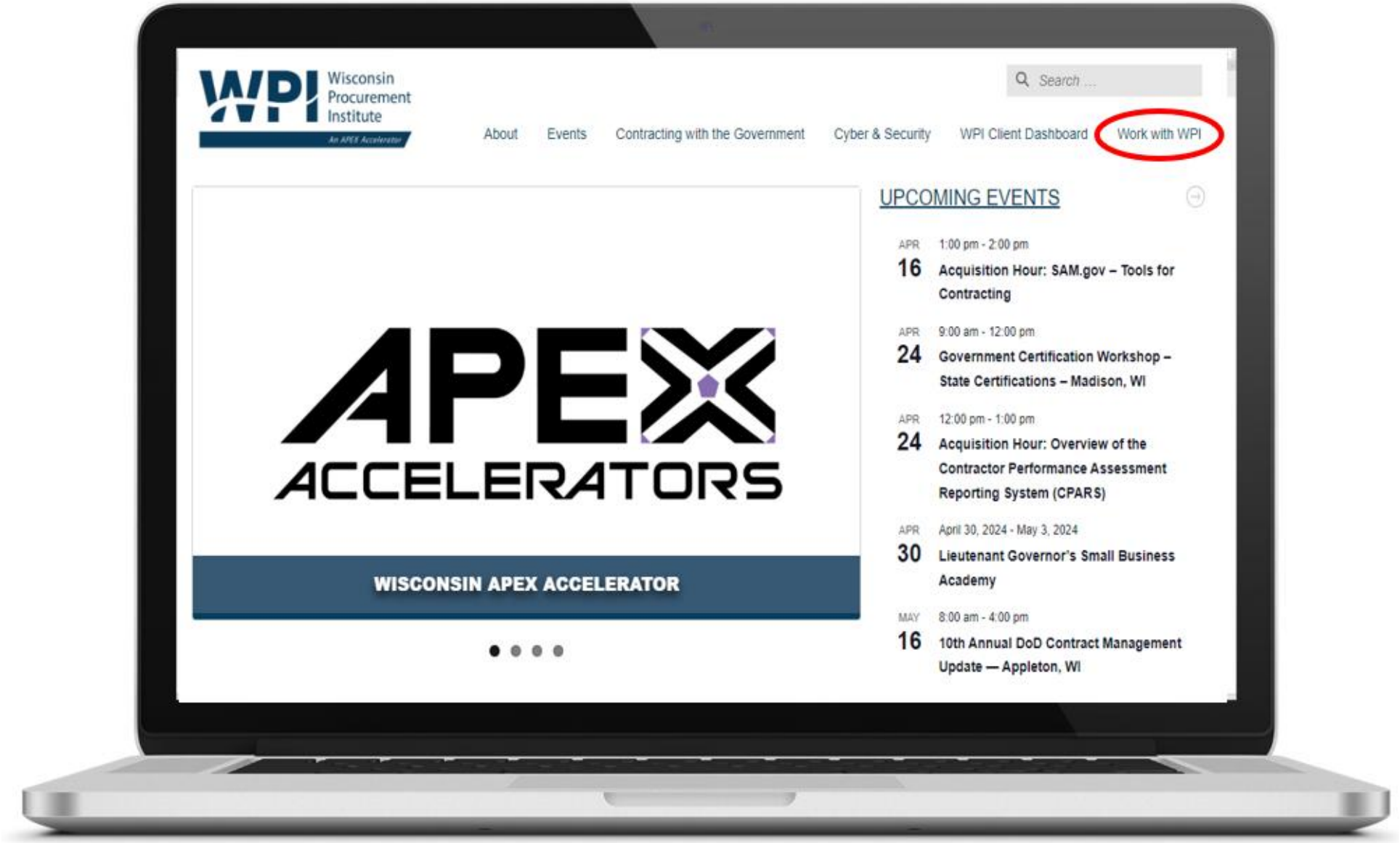
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting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

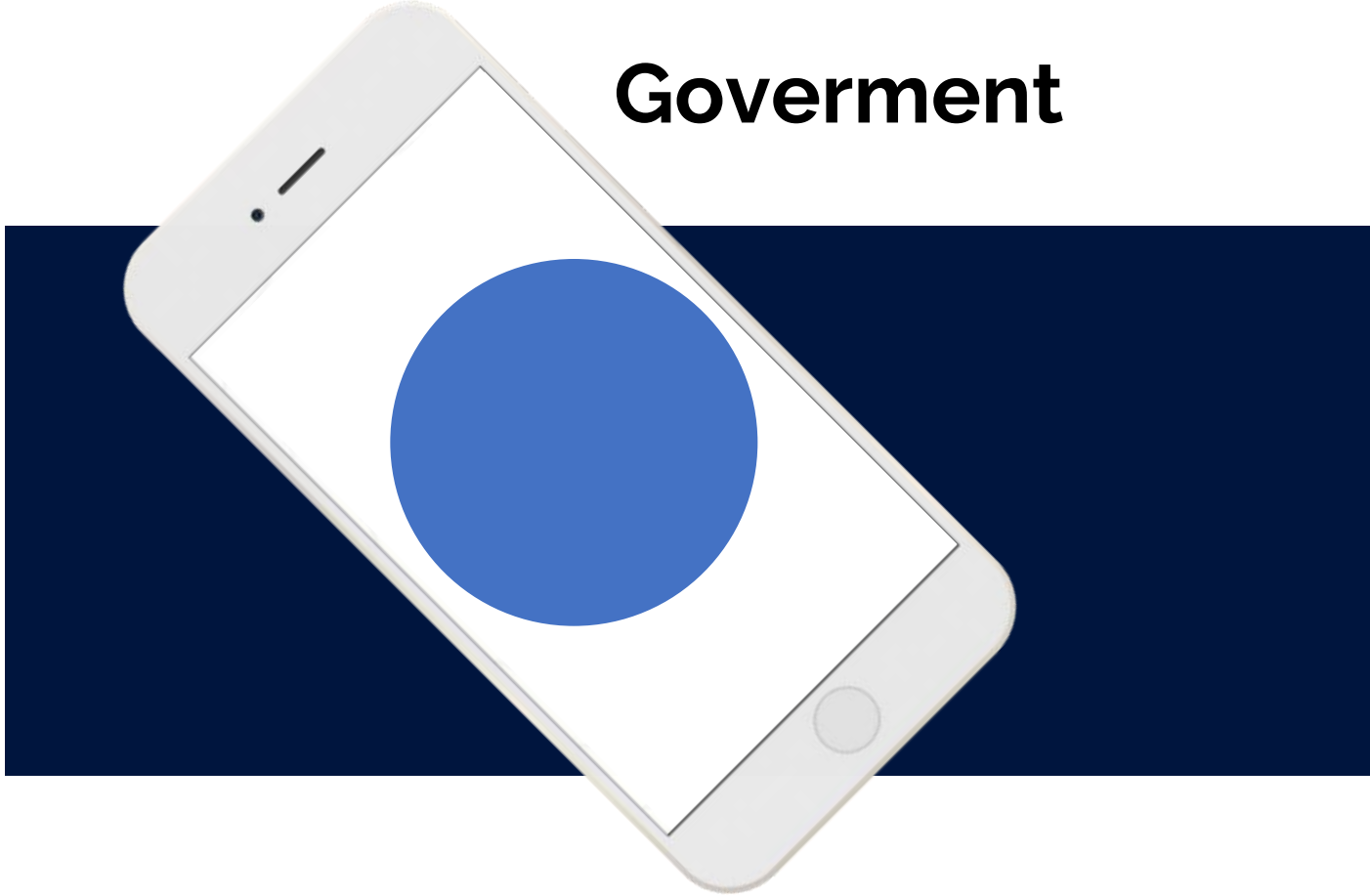



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 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

Rules You Need to Know to Work With the Federal Goverment

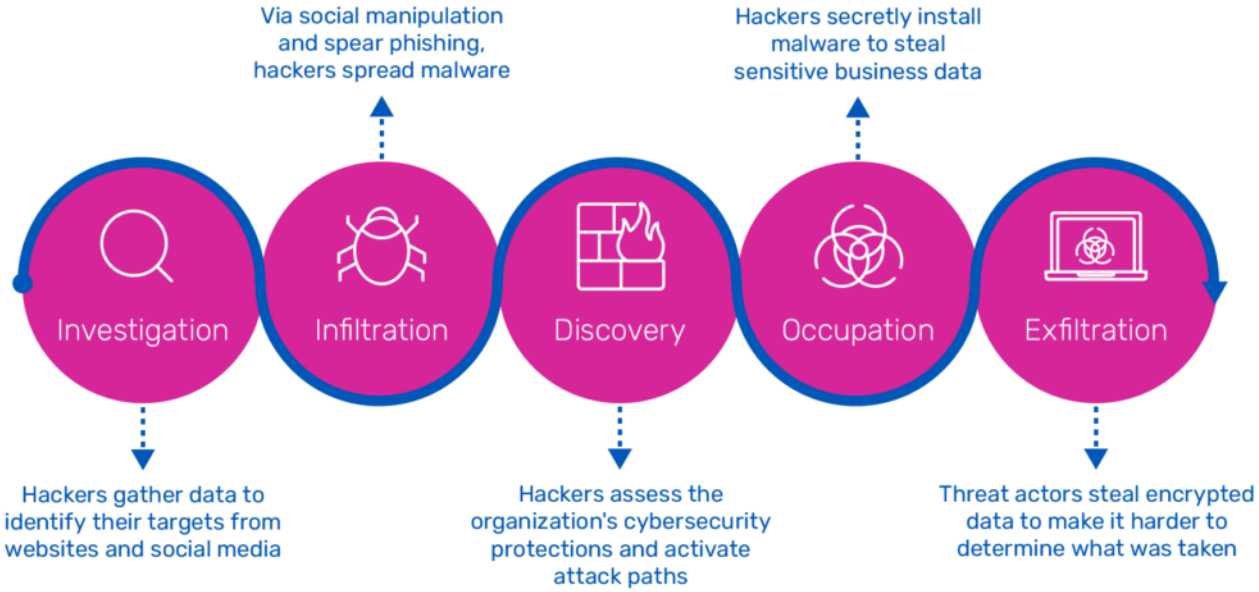
Wisconsin Procurement Institute

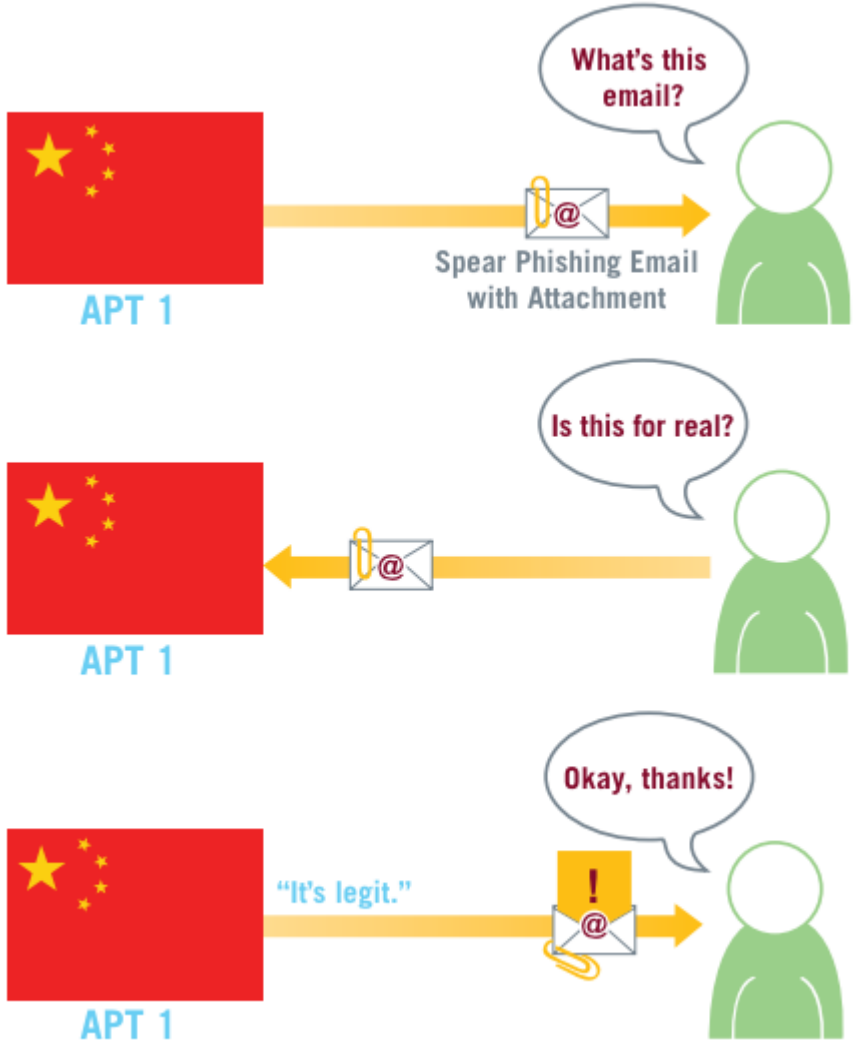
AN APEX ACCELERATOR



May 30th, 2025

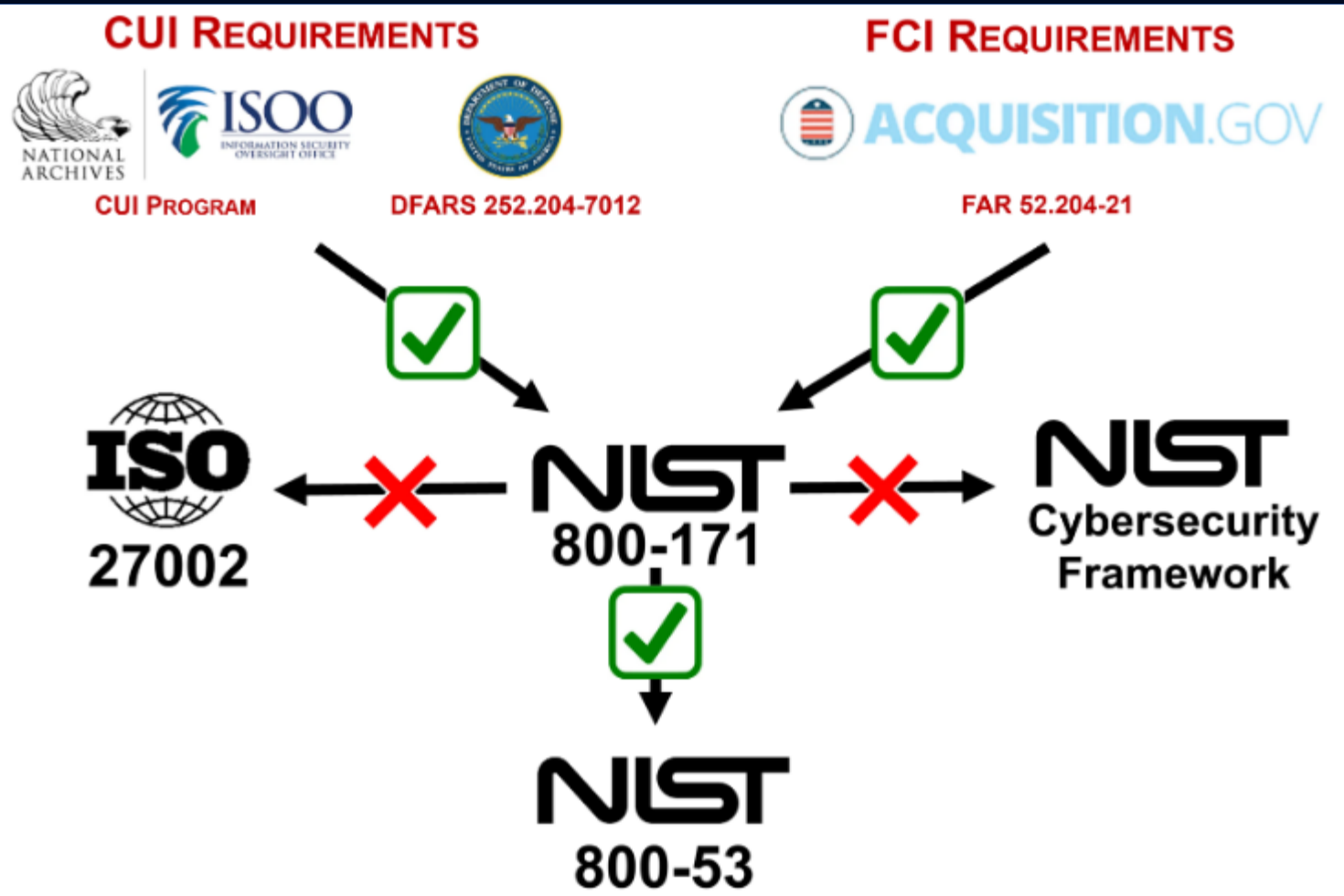
What is an Advanced Persisent Threat?






LOCKHEED MARTIN
3103

FAR 52.204-21, DFARS, NIST, and Beyond



An Evolution – Not a Departure

Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

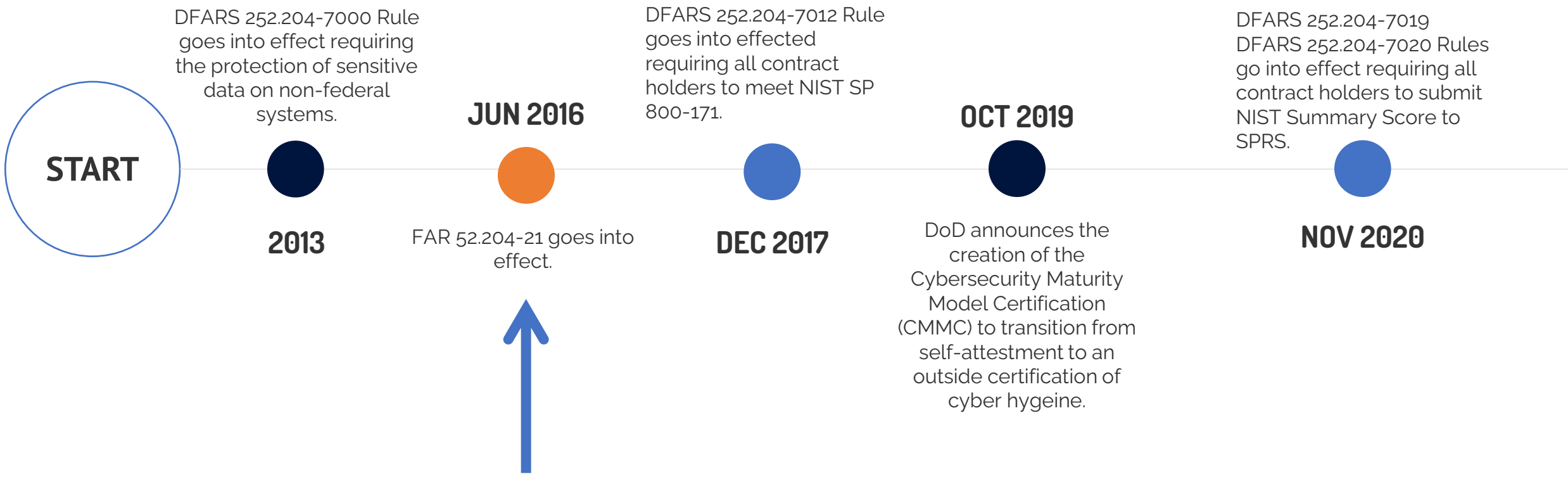
DFARS 252.204-7021

ACQUISITION.GOV

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

1. 15 Controls
2. Self-Attestation
3.

Cybersecurity Timeline



What is FCI?

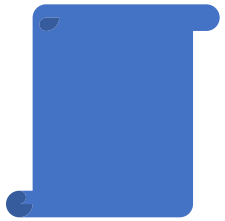
Federal contract information (from 48 CFR 52.204-21) means information, not intended for public release, that is **provided by or generated for the Government under a contract to develop or deliver a product or service to the Government**, but not including information provided by the Government to the 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 requirements and procedures to protect covered contractor information systems.

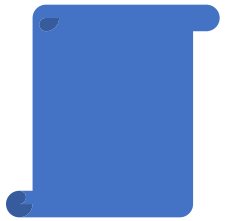
Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Key Points



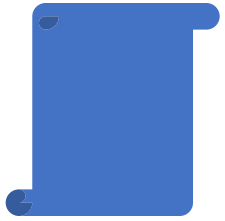
15 Controls

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



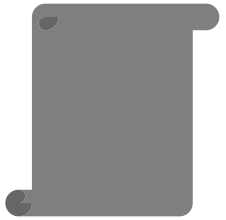
Are Echoed within NIST SP 800-171 Requirements

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



Considered Introductory

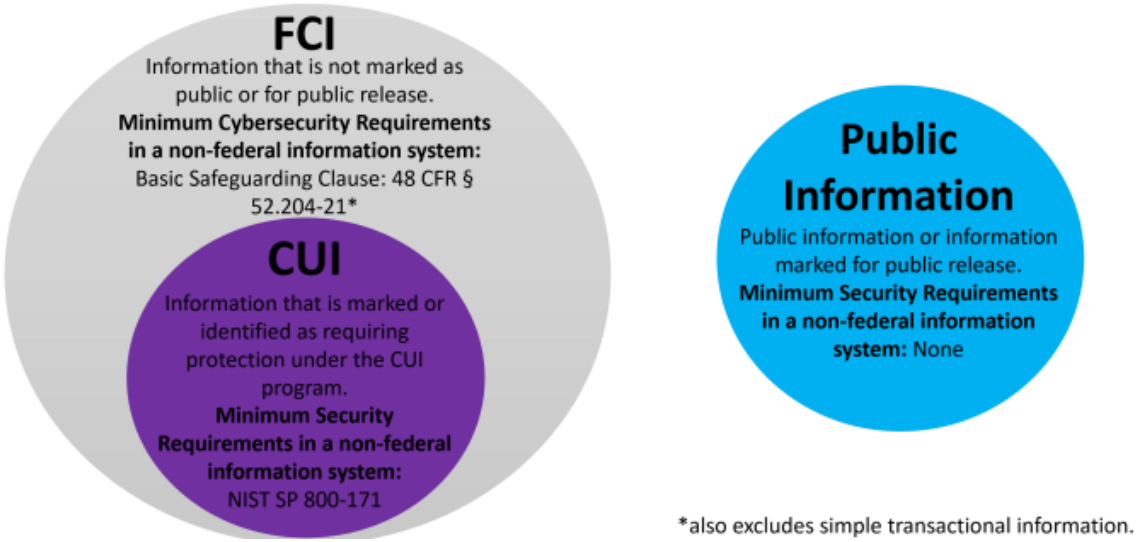
These controls represent minimal efforts, expense, and expertise to apply. “Common Sense” security.



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

ACQUISITION.GOV

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

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

Cybersecurity Timeline

START

2013

DFARS 252.204-7000 Rule goes into effect requiring the protection of sensitive data on non-federal systems.

JUN 2016

FAR 52.204-21 goes into effect.

DEC 2017

DFARS 252.204-7012 Rule goes into effected requiring all contract holders to meet NIST SP 800-171.

OCT 2019

DoD announces the creation of the Cybersecurity Maturity Model Certification (CMMC) to transition from self-attestment to an outside certification of cyber hygeine.

NOV 2020

DFARS 252.204-7019
DFARS 252.204-7020 Rules go into effect requiring all contract holders to submit NIST Summary Score to SPRS.

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

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.

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.

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 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.

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

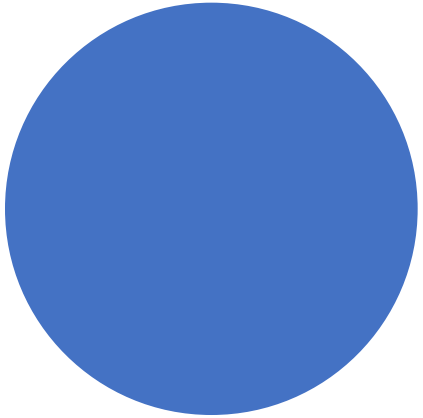
NIST SP 800-171A

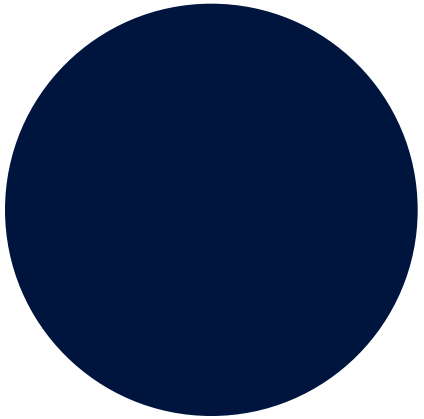
3

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

Plan of Action and Milestones

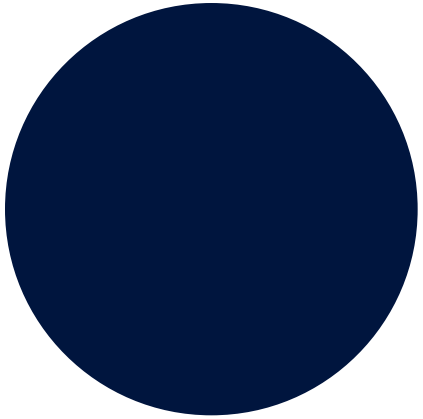
Tasks that need to be accomplished

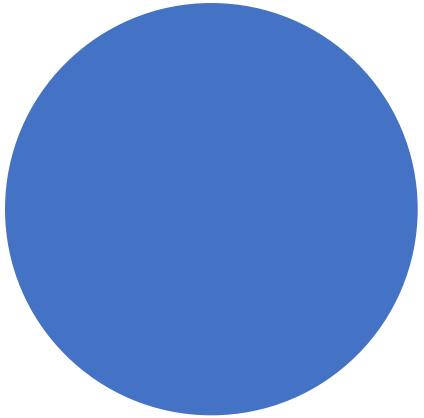




Milestones for meeting the tasks

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

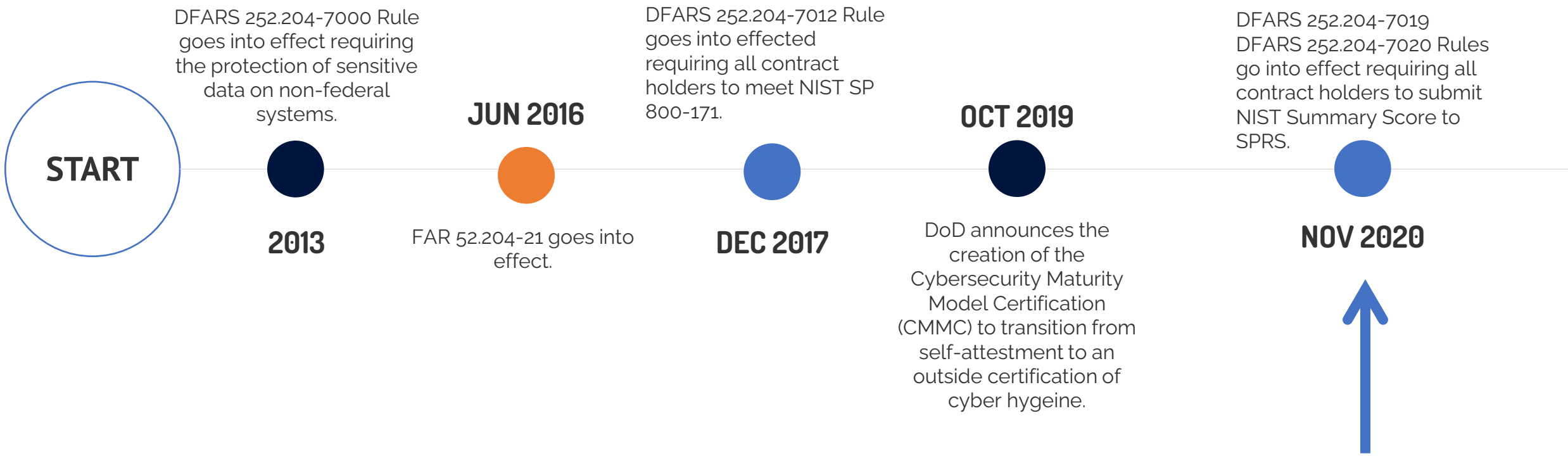
FAR 52.204.-21

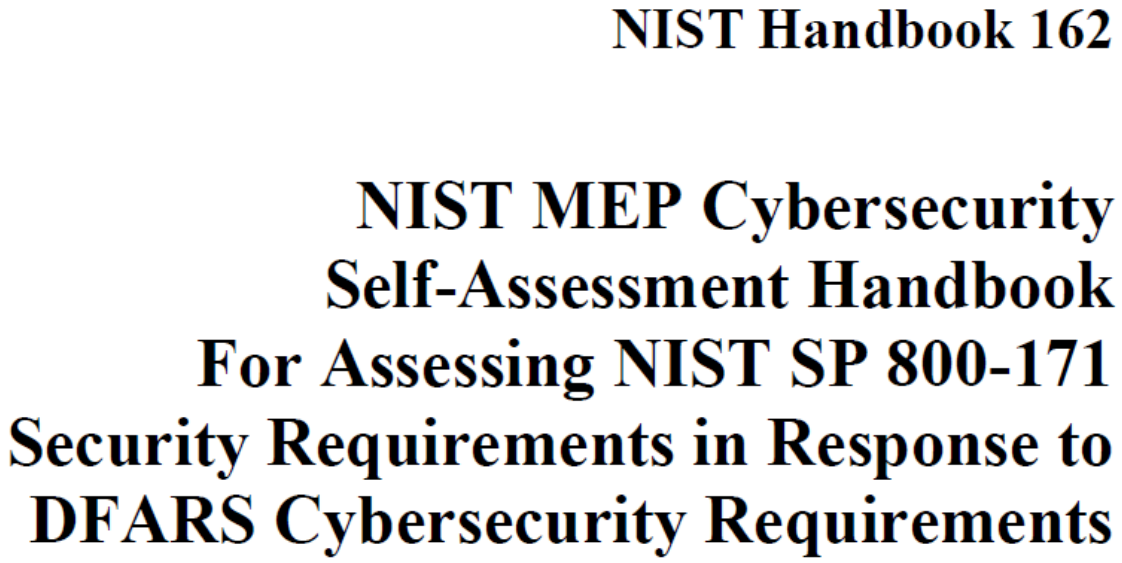
DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021

Cybersecurity Timeline





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

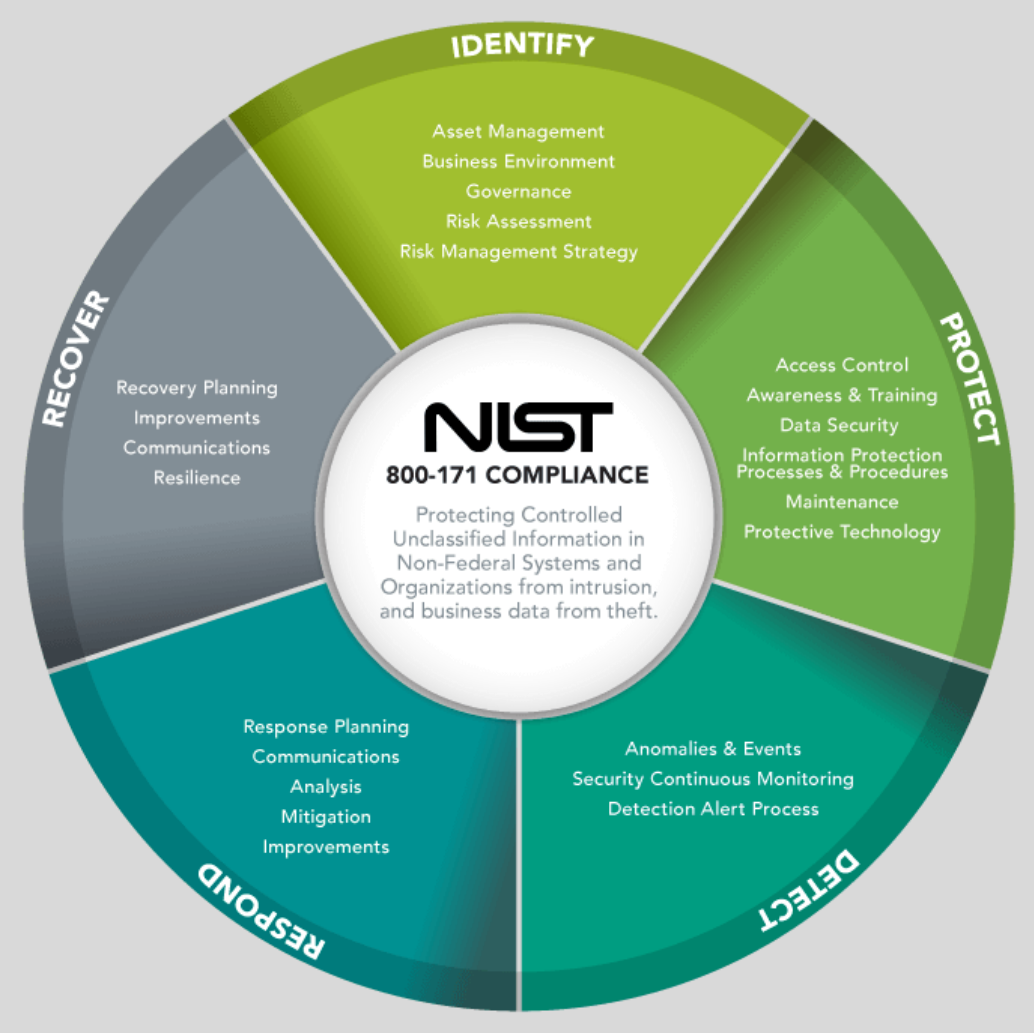
3

DoD Memo

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

DFARS 252.204-7019

NIST SP 800-171 DOD Assessment Requirements
(Provision)



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

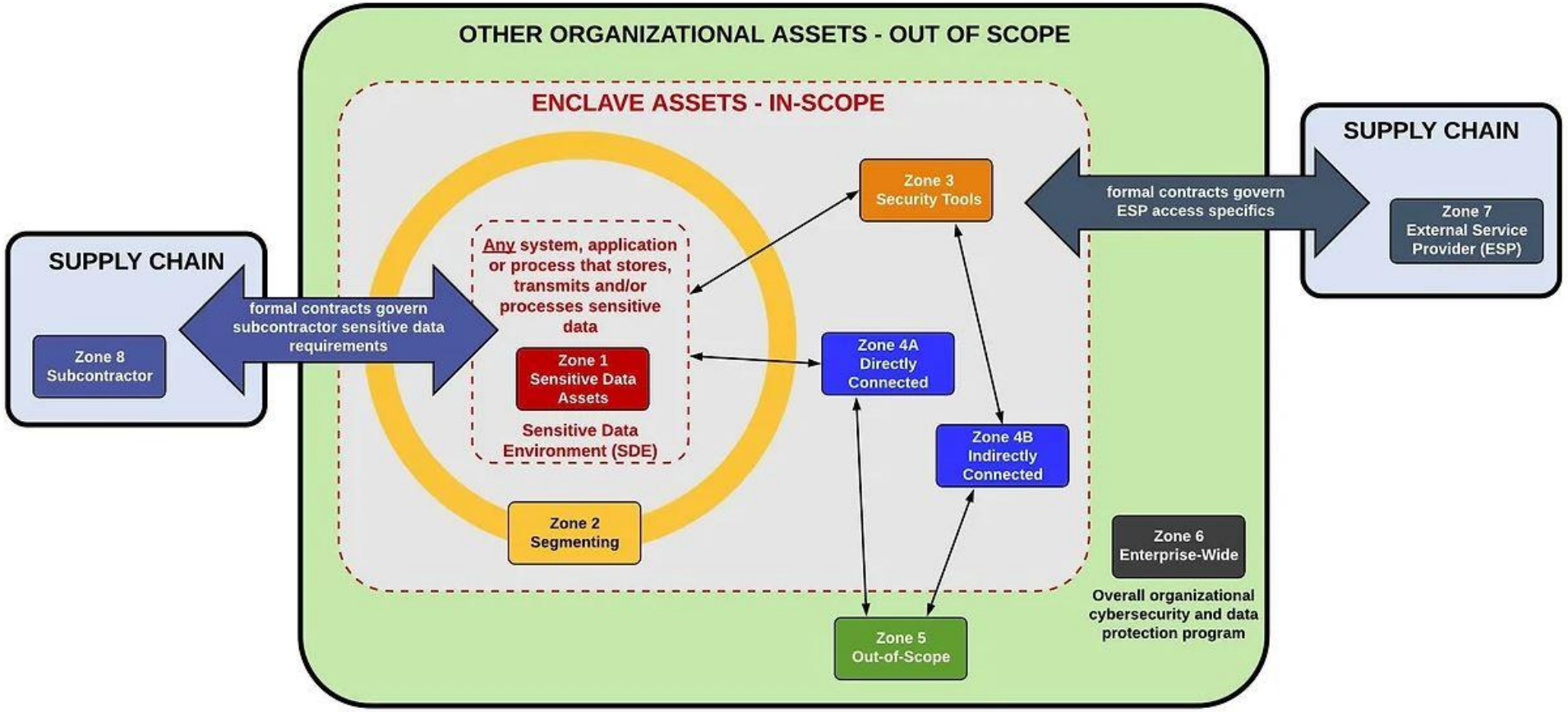
Why a Self-Assessment?

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.

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 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 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

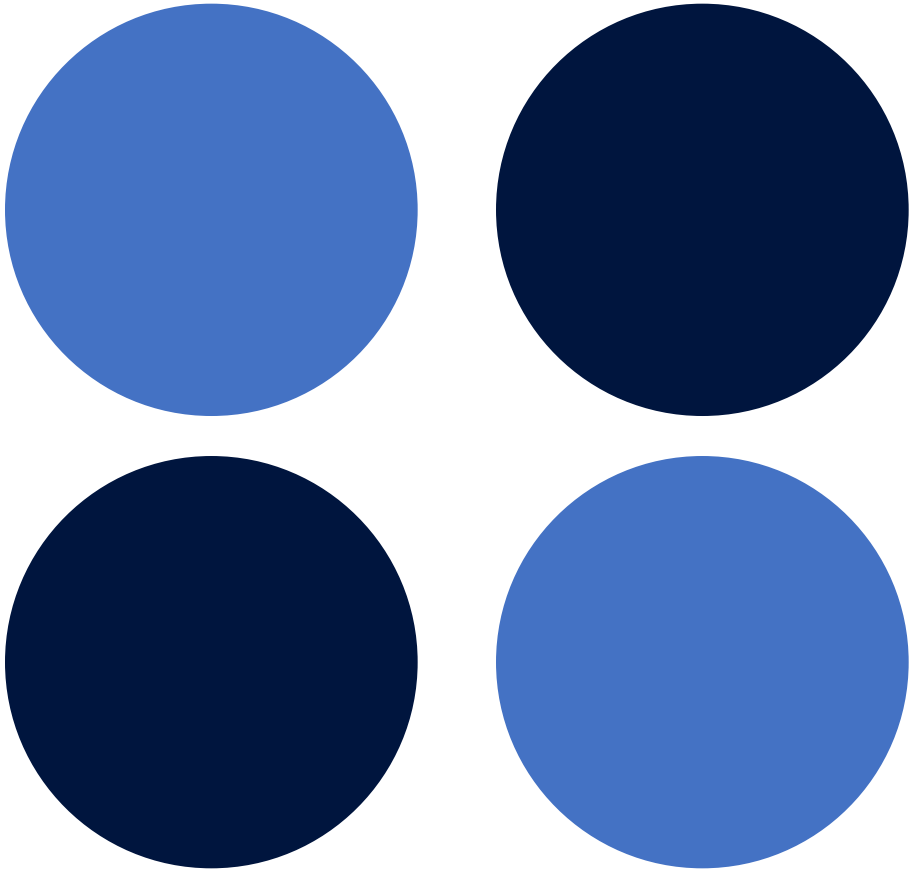
Perform Test On:

- automated mechanisms implementing information flow enforcement policy

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].

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.

FIPS 199

1.3 Information Owner

1.3.1	Name		☐
1.3.2	Title		☐
1.3.3	Office Address		☐
1.3.4	Work Phone		☐
1.3.5	E-Mail Address		☐

1.4 System Security Officer

1.3.1	Name		☐
1.3.2	Title		☐
1.3.3	Office Address		☐
1.3.4	Work Phone		☐
1.3.5	E-Mail Address		☐

1.5 General Description/Purpose of System

1.5.1	Description	Test Company's IT For CUI	☐
1.5.2	Number of Users/Privileged Users		☐
1.5.3	Description of Information		☐

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

Regulations

FAR 52.204.-21

DFARS 252.204-7012

DFARS 252.204-7019/7020

DFARS 252.204-7021

Cybersecurity Timeline

OCT 2024

32 CFR Part 170 published for comment – establishment of CMMC Program.

DEC 2024

32 CFR Part 170 finalized – establishment of CMMC Program.

JUN 2025?

Anticipated Publishing of 48 CFR – enforcing CMMC Requirements on Contracts/Solicitations.

Spring 2026?

The CMMC Final Rule was published on **October 15, 2024**. It **BECAME** effective on **Dec 16, 2024**, and can now enter contracts and solicitations. Most are anticipated in **mid-2025** (Q2, March-April anticipated).

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

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**.

Supplier Performance Risk System

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

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.

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.

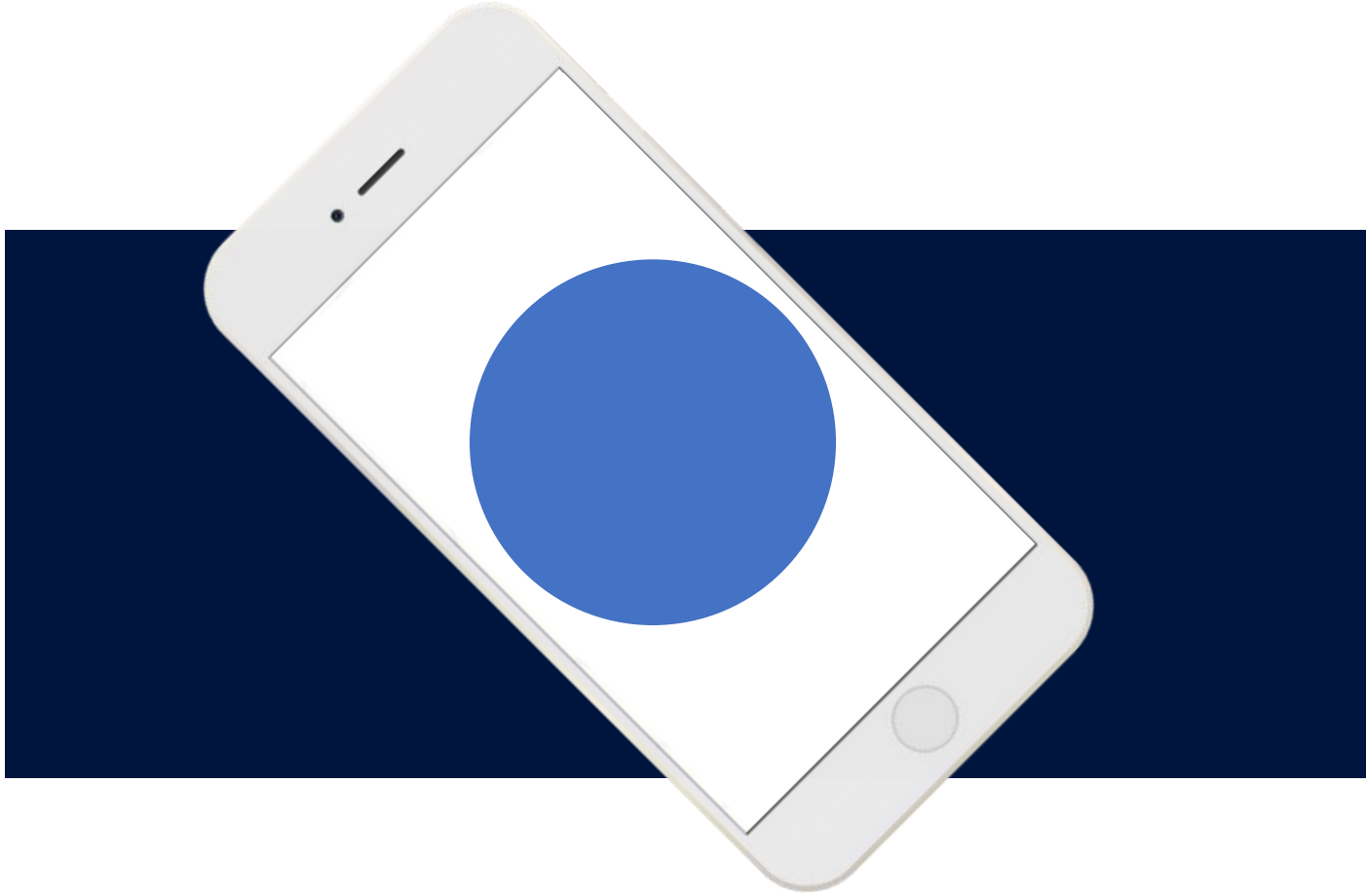
If the overall scoring of the Assessment after placing items on the Limited Practice Deficiency Correction program results in **greater than or equal to 80%** (88/110 practices “MET”), the OSC will be required to correct deficiencies.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR



Upcoming Events

Cyber Friday

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.

- **May 30** - Cybersecurity Rules You Need to Know to Work with the Federal Government / Department of Defense

More dates to be announced soon!

…More information and registrations at wispro.org/events

19th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In Partnership with Wisconsin's Military Installations

June 18
Volk Field ANGB

July 9
Truax Field

July 30
Fort McCoy

GOBC will provide you the opportunity to gain insights into:

- ***COFFEE with the COMMANDER***
- Current operations and priorities at Wisconsin's Federal and State government agencies and military facilities
- Connecting with agency and installation leadership, operational staff and buyers
- Locating and bidding on current and future procurement opportunities
- Resources available to assist your business in winning government prime and subcontracts

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

May 30 2025

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

mattf@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226