Cyber Friday:

CMMC: Are You Ready for a C3PAO Assessment?

March 28 | 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.

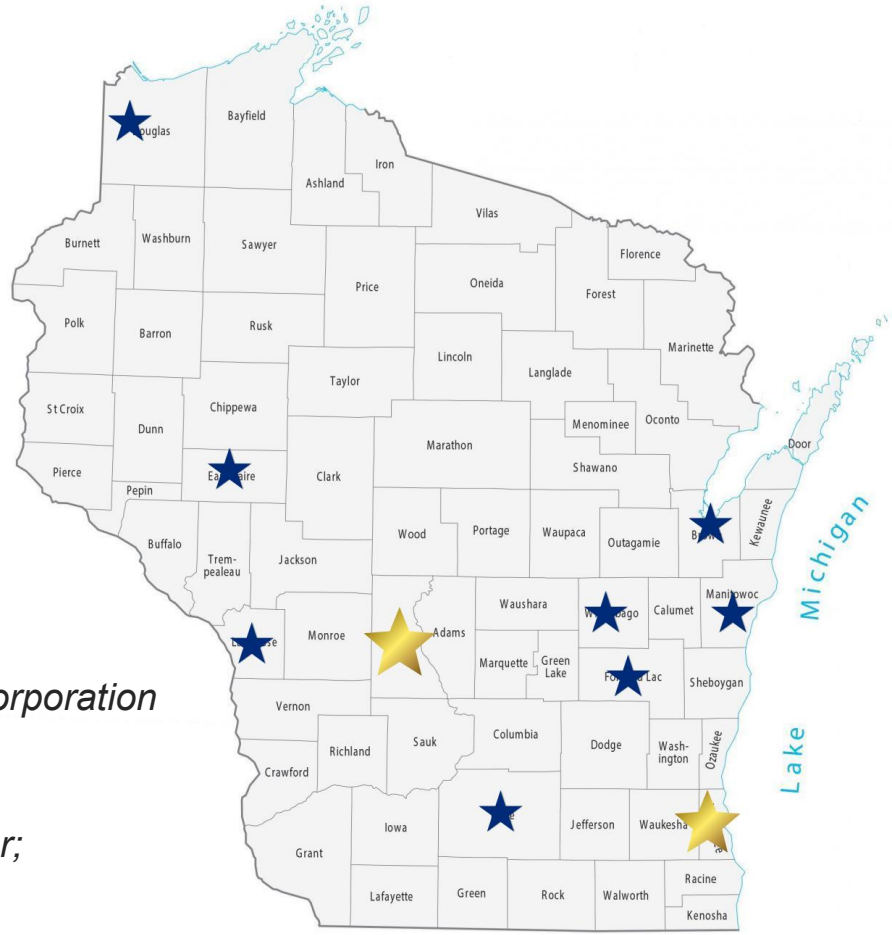
WPI provides services and training to all of Wisconsin's 72 counties

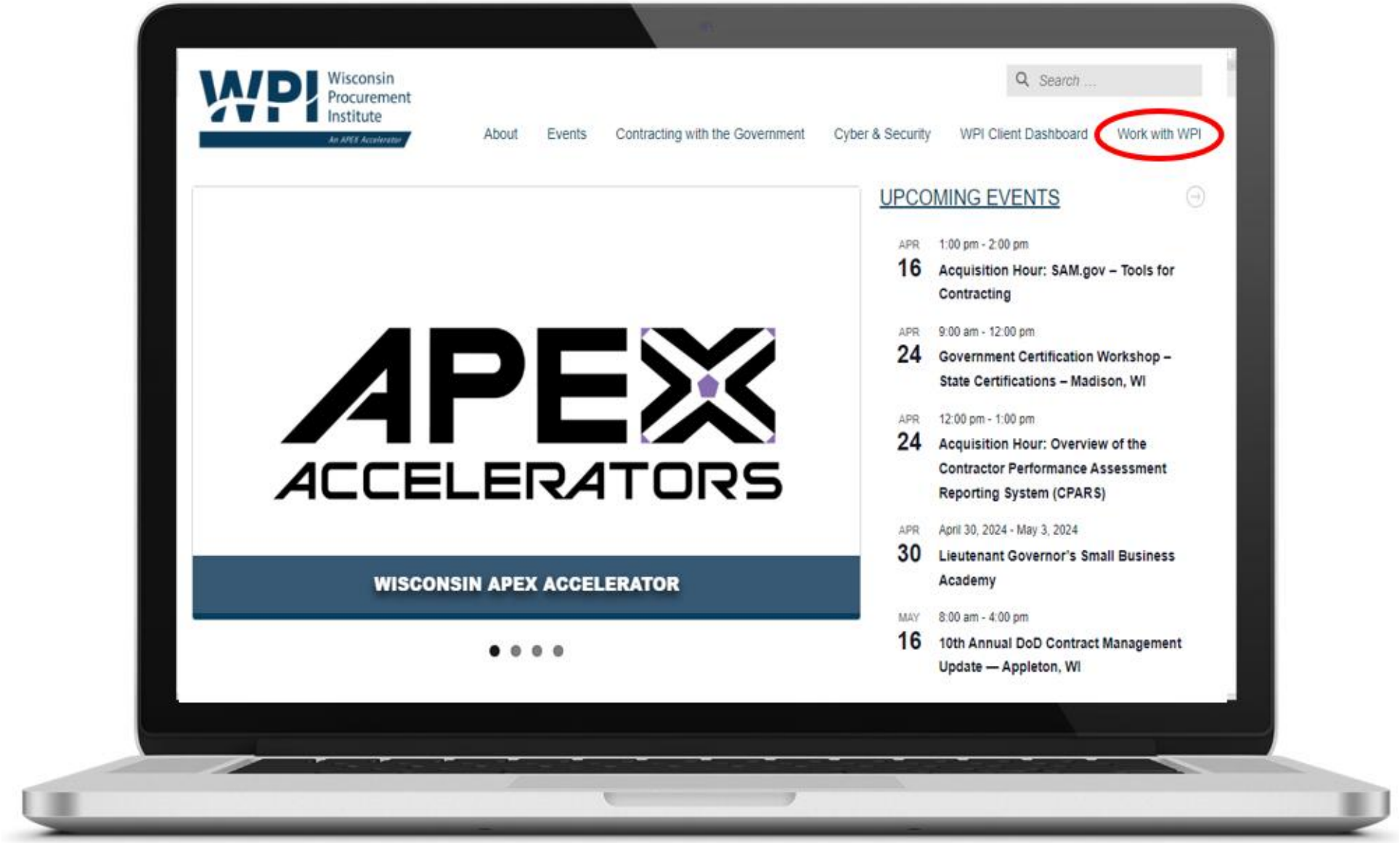
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting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

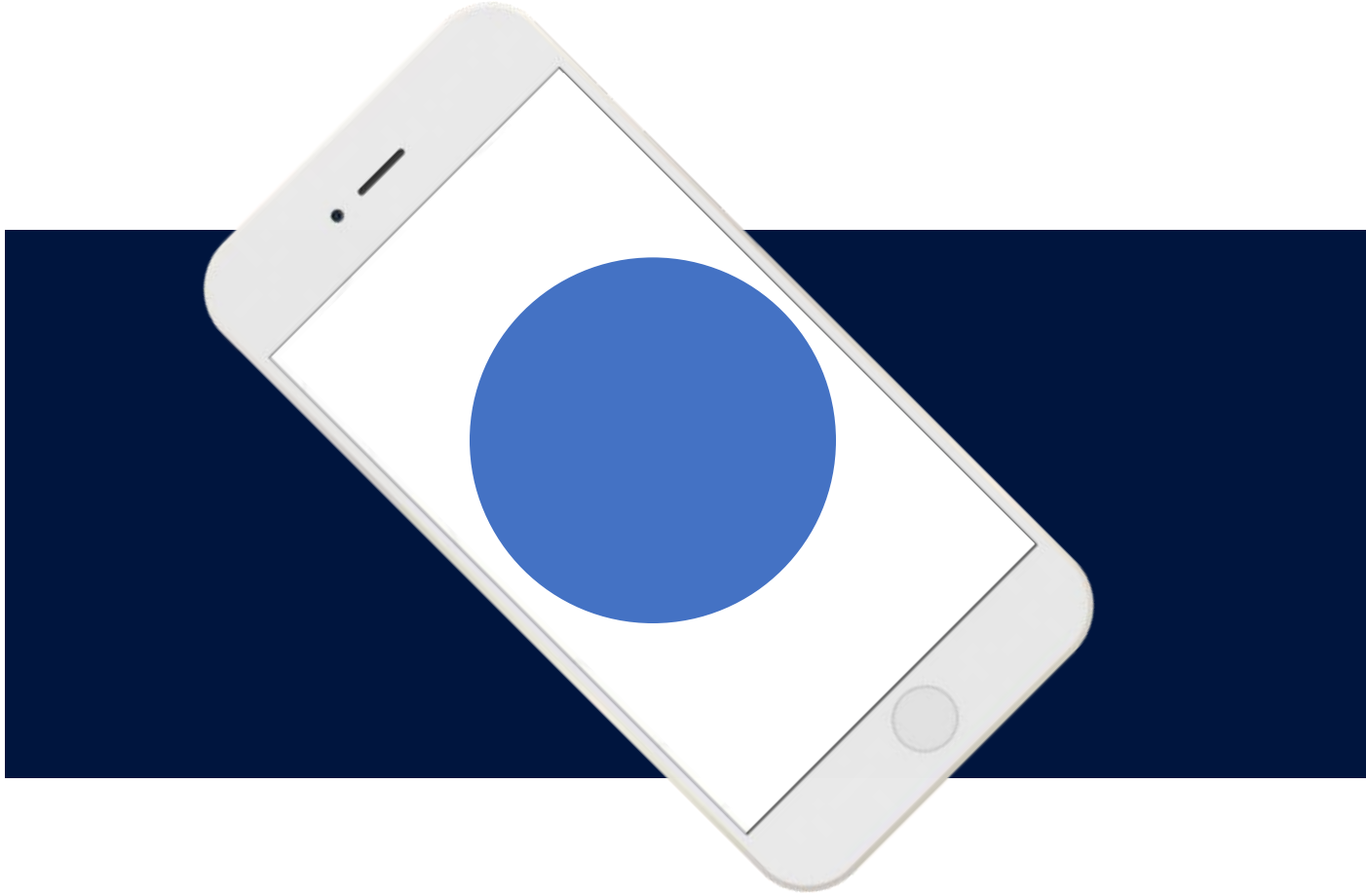



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR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

Are You Ready for a C3PAO Assessment?

Wisconsin Procurement Institute

An APEX Accelerator



CYBER FRIDAY SESSIONS – March 28th, 2025

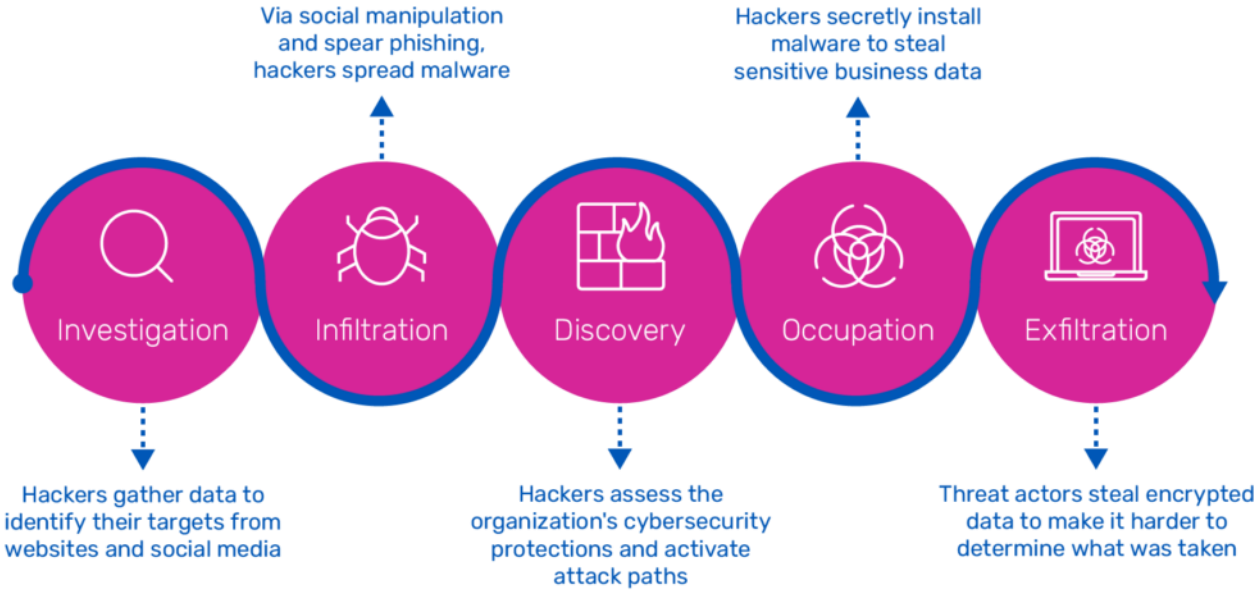
Confirmed in 2013, the theft of data from the F-35 Lightning II represented one of the most significant data breaches in world history.

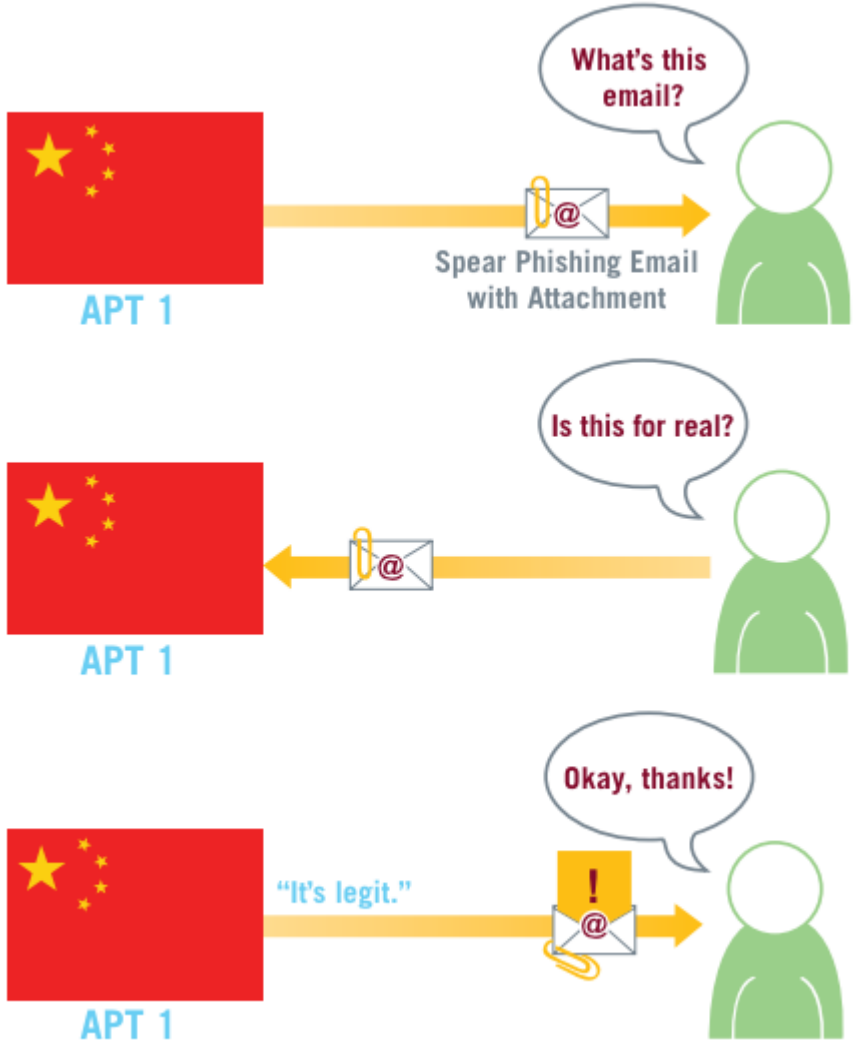
Breach involved a series of units, funded and operated by the PLA, identified as Advanced Persistent Threats (APT).

Targets were companies within Lockheed Martin's supply chain.

Data was primarily unclassified, but controlled, information.

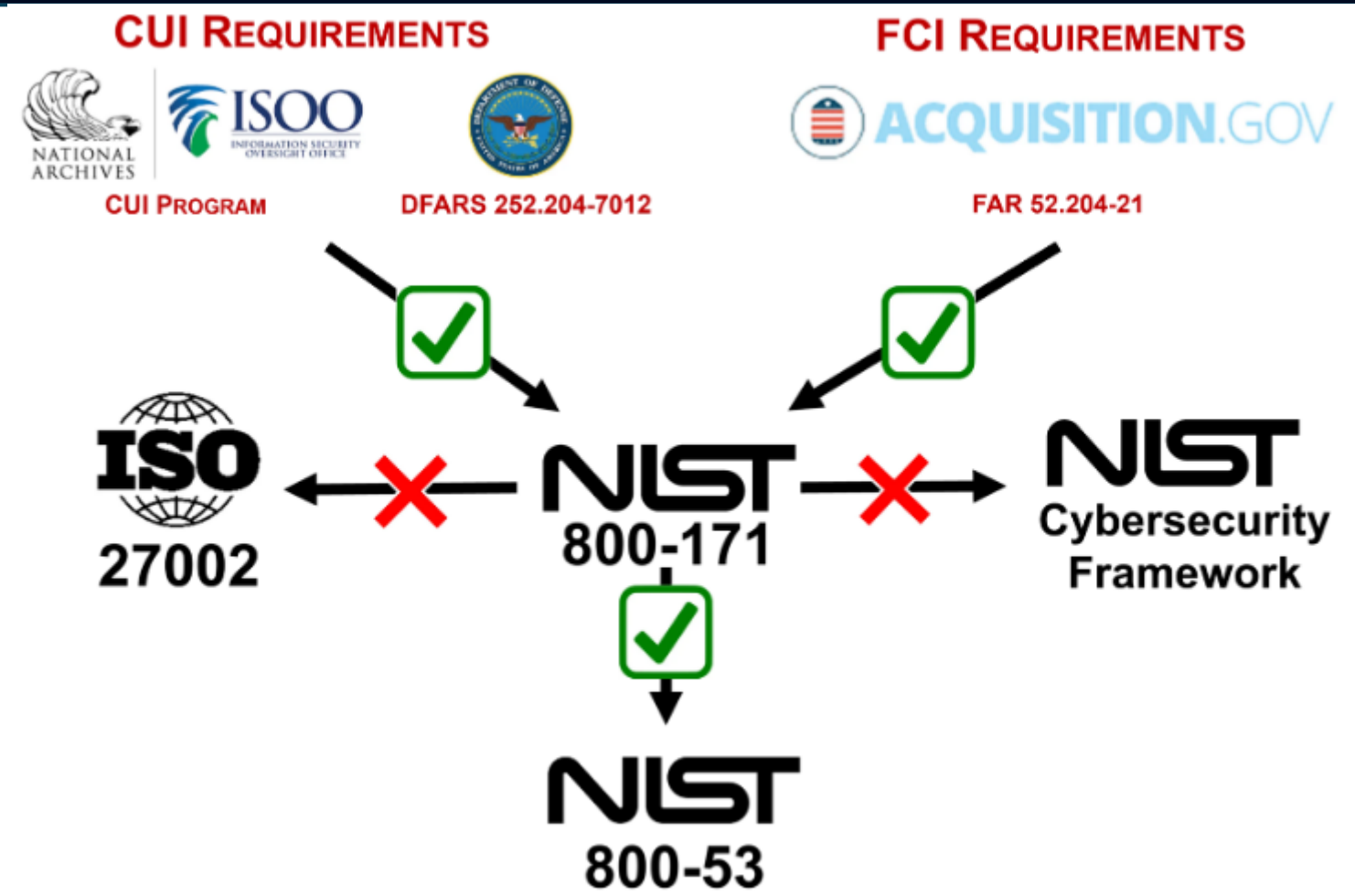
What is an Advanced Persisent Threat?





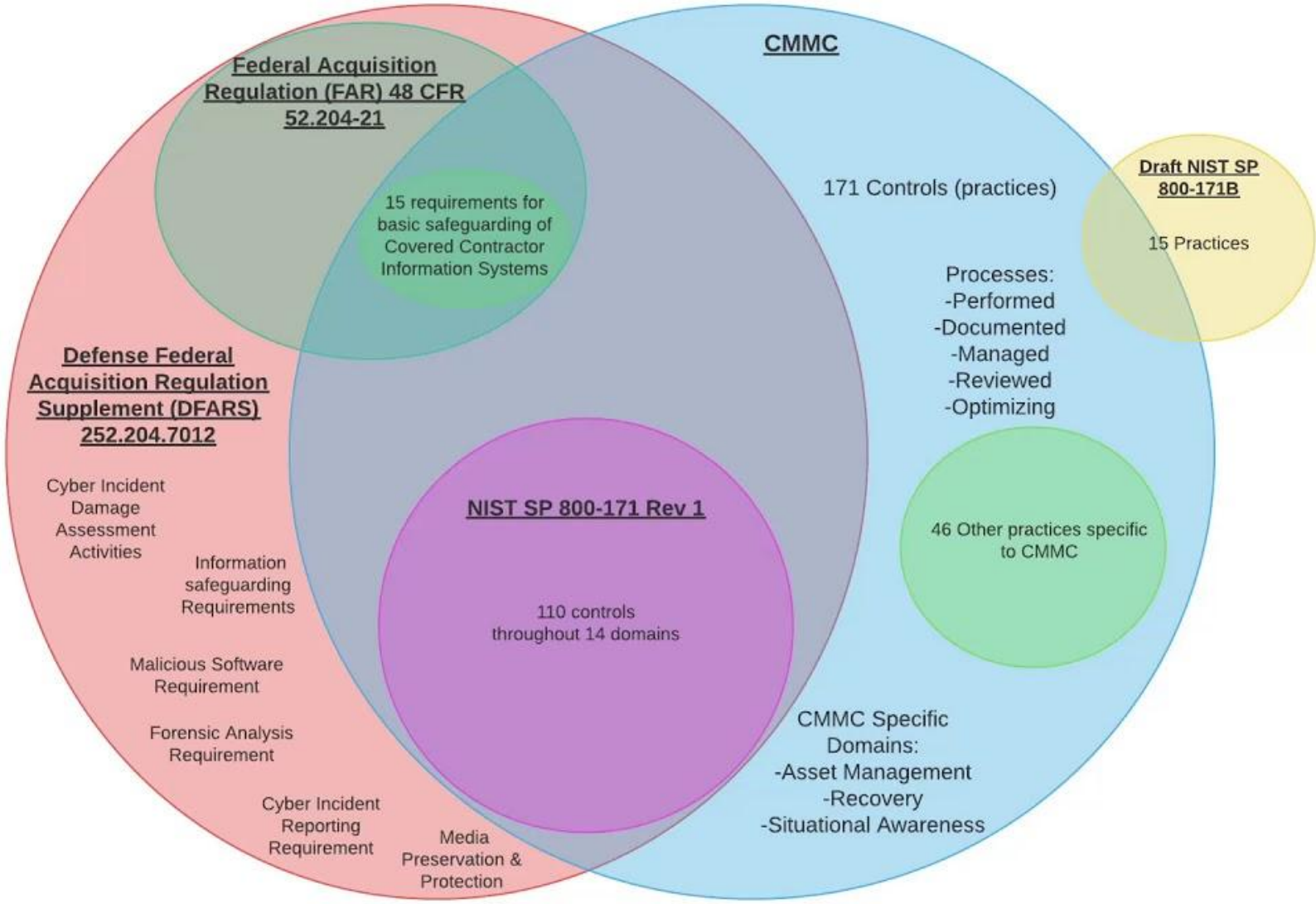

LOCKHEED MARTIN
3103

FAR 52.204-21, DFARS, NIST, and Beyond



An Evolution – Not a Departure

FAR 52.204-21, DFARS, NIST, and Beyond



DFARS 252.204-7012

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.

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

DFARS 252.204-7021

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.

The Jist

ACQUISITION.GOV

NIST
National Institute of Standards and Technology

The Regulations

FAR / DFAR

The Standard

The Assurance

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).

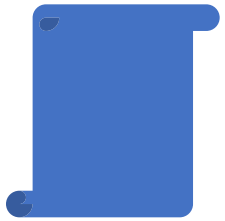
Supplier Performance Risk System

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

What is FCI?

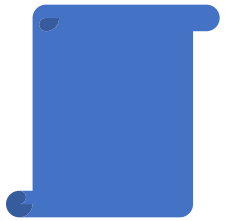
Federal contract information (from 48 CFR 52.204-21) means information, not intended for public release, that is **provided by or generated for the Government under a contract to develop or deliver a product or service to the Government**, but not including information provided by the Government to the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

Key Points



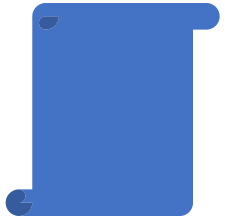
15 Controls

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



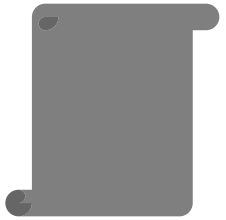
Are Echoed within NIST SP 800-171 Requirements

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.

Supplier Performance Risk System

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

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.

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**.

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)

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.

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.

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)

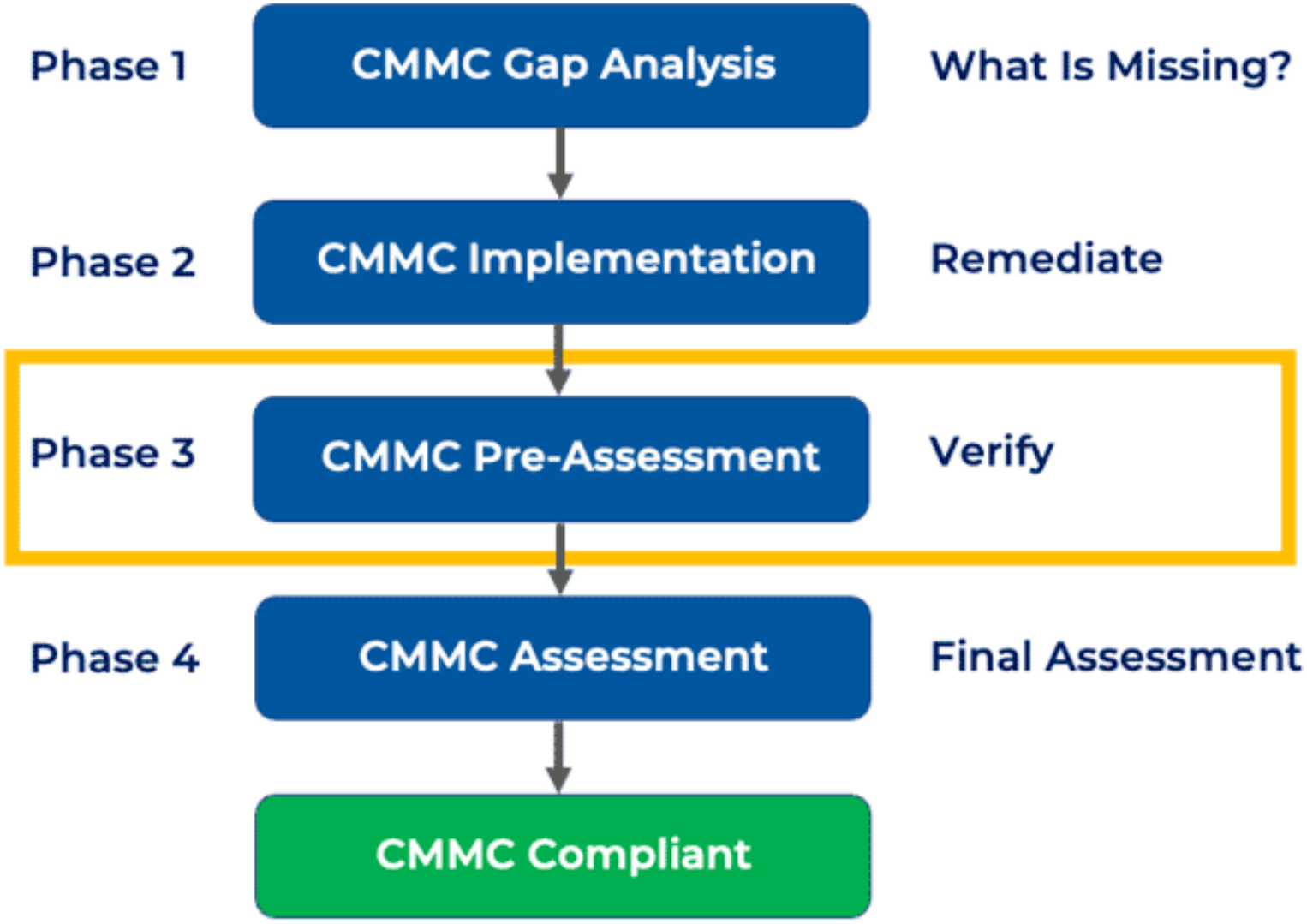
WPI Wisconsin Procurement Institute

APEX ACCELERATORS

CMMC Quick Check

Review for Obvious Deficiencies	Complete	Comments
Has the SSP been reviewed?		
Have data flow diagrams been reviewed?		
Have network diagrams been reviewed?		
Has the last self-assessment report and plan been reviewed?		
Has the device inventory been reviewed?		
Has the software inventory been reviewed?		
Has personnel inventory been reviewed?		
Has each external service provider been inventoried and reviewed?		
Has the FIPS documentation been reviewed?		
Have all “N/A” and “alternate implementation” practices been reviewed?		
Are applicable practices described for each system?		
Have all in-scope external service providers been reviewed to ensure they have audit reports suitable for inheritance, or will attend assessment?		
Are all customer responsibilities met and described for in-scope external service providers?		

CMMC Assessment Timeline



Select C3PAO and Schedule

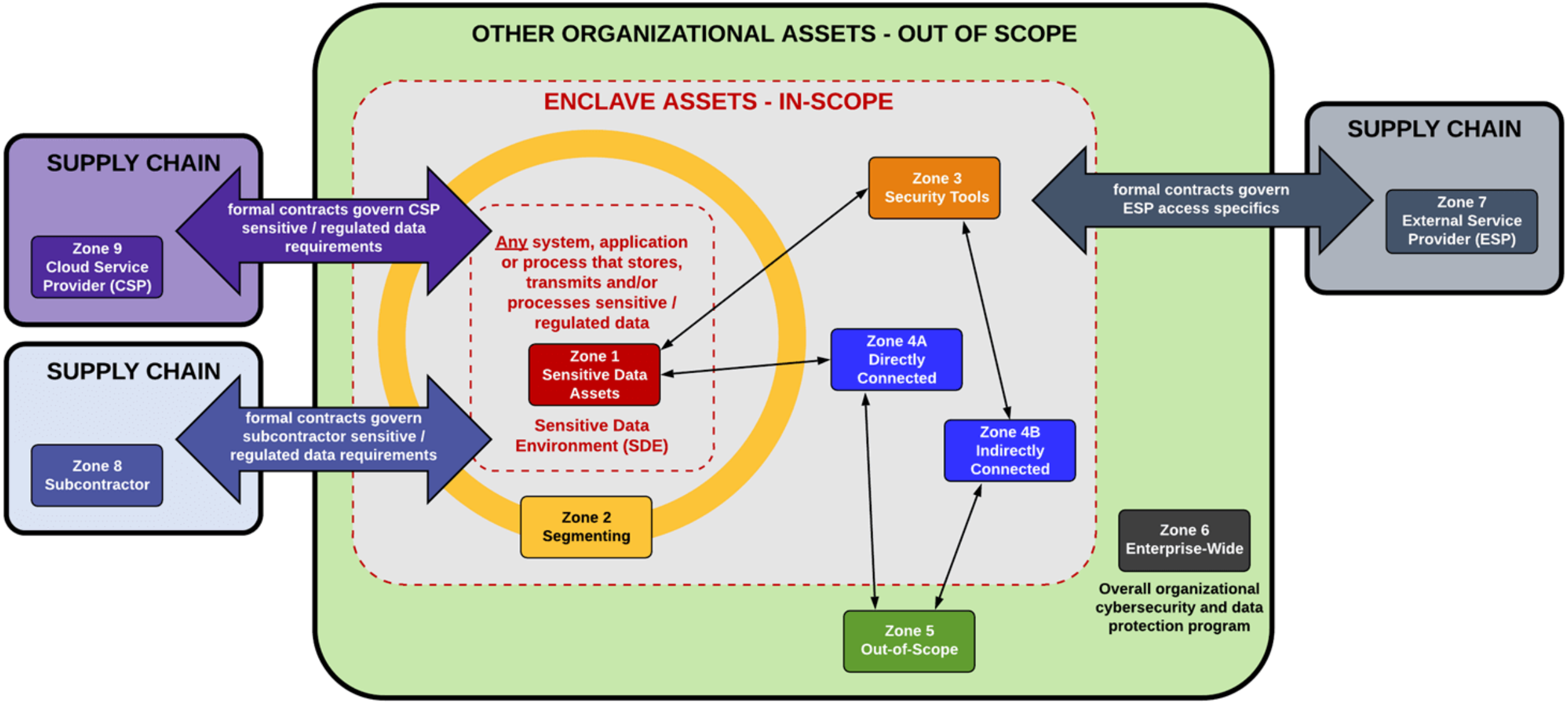
ABOUT US ▾ ACCREDITATION ▾ RESOURCES ▾ CMMC ECOSYSTEM ▾ NEWS & EVENTS ▾ MARKETPLACE CAICO

www.cyberab.org

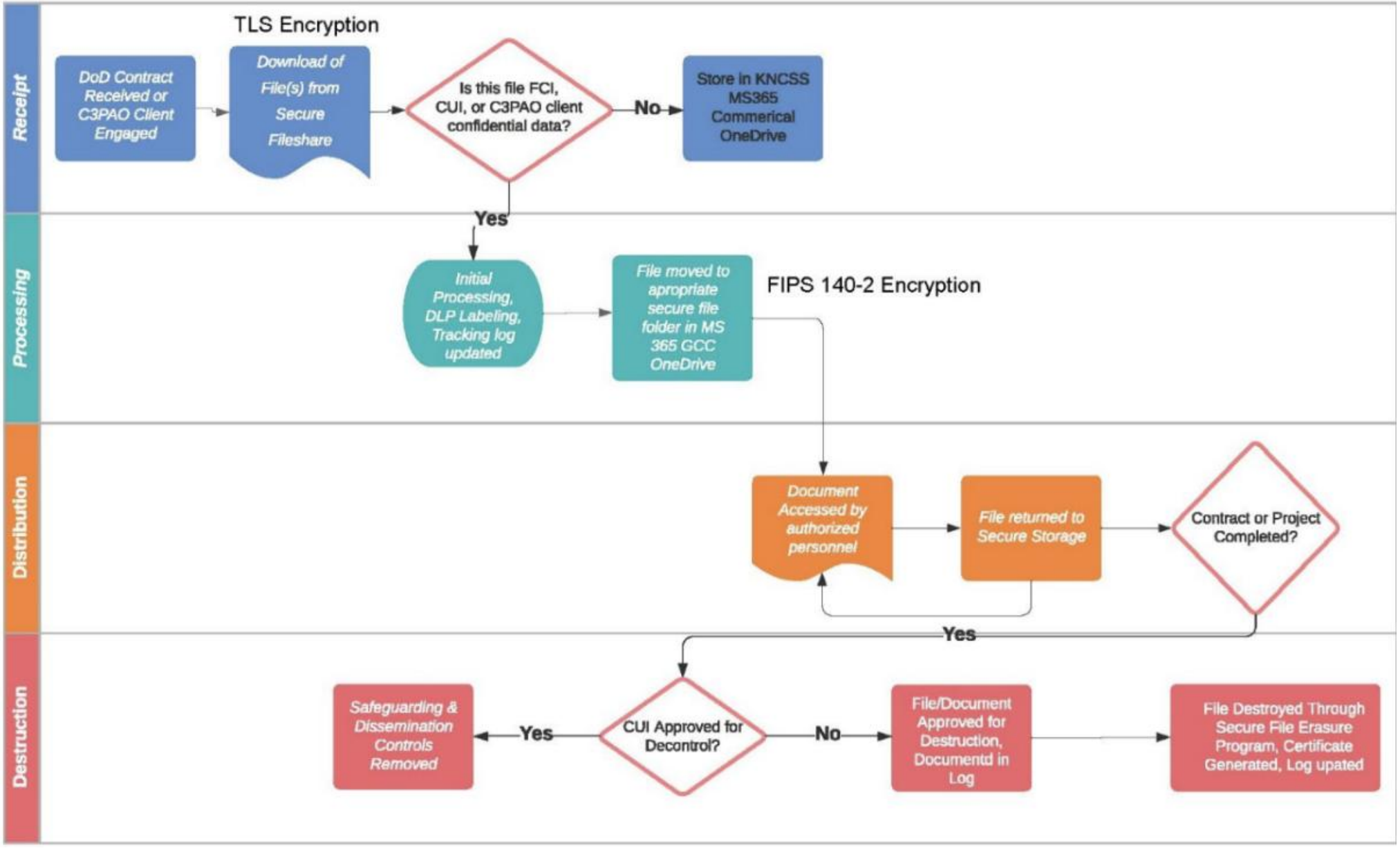
CMMC L2 Assessment Phases

1. Plan and Prepare the Assessment
2. Conduct the Assessment
3. Report Assessment Results
4. Close-Out POA&Ms and Assessment

Define Scope of Assessment



CUI Data/Process Flow



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.

1. Assessment

1. Schedule the Assessment

2. Receive Assessment Plan
   Typically, 5 Days
   End of Day Hotwash of Day's Findings

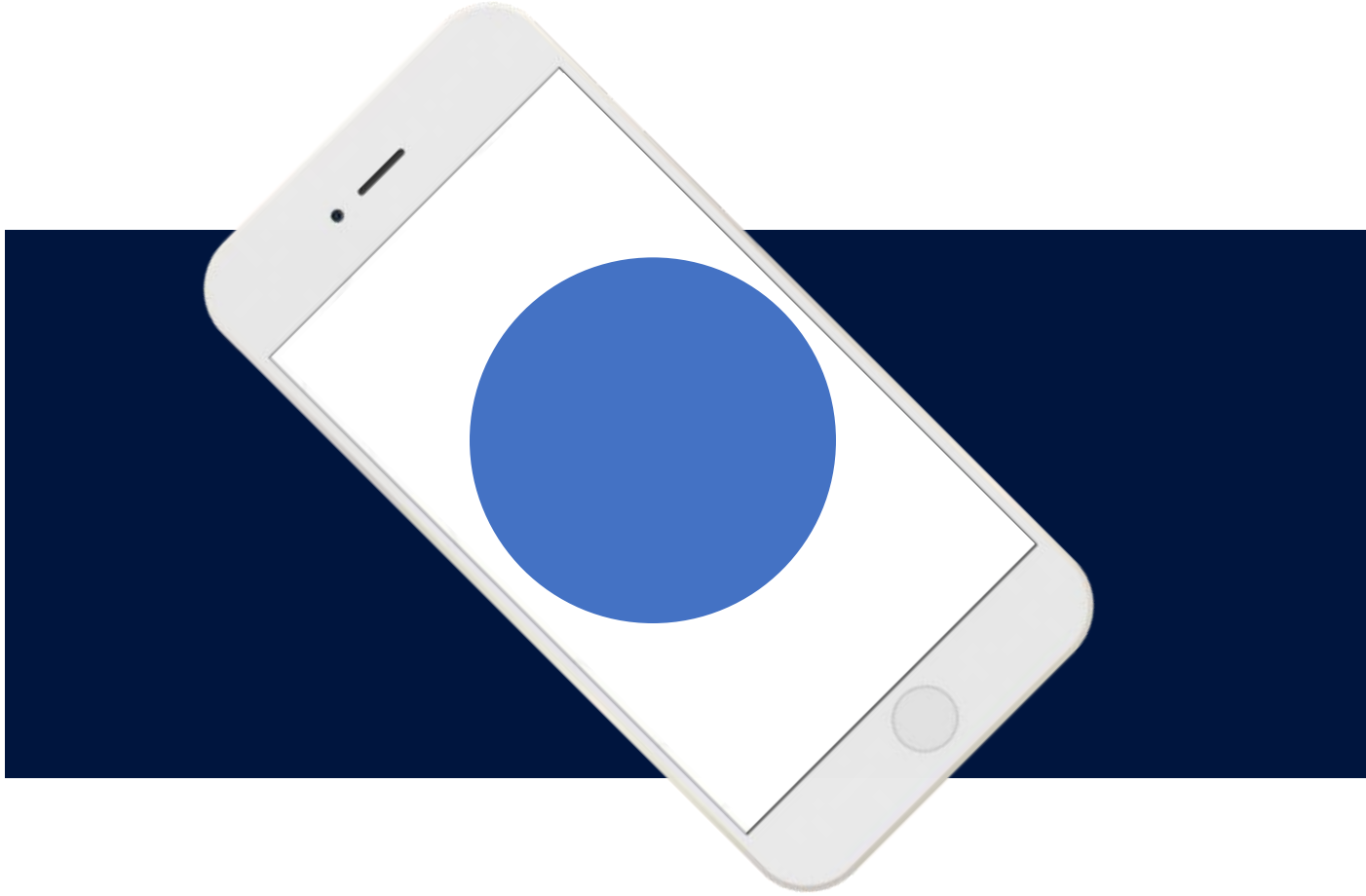
3. Will Likely Have OnSite Component

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.

- **March 28** – CMMC: Federal Cybersecurity Requirements – Who Must Comply?
- **April 25** – CMMC: Maintaining Your CMMC Certification

…More information and registrations at wispro.org/events

Upcoming Events

May 14

Winning Government Business: Navigating Compliance Risks to Drive Strategic Advantage

Milwaukee, WI

May 15

11th Annual DOD Contract Management Update

Milwaukee, WI

…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

March 28 2025

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