Wisconsin Procurement Institute

An APEX Accelerator

Acquisition Hour:
CMMC Update – October 2024

October 25| 1:00 – 2:00 pm

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

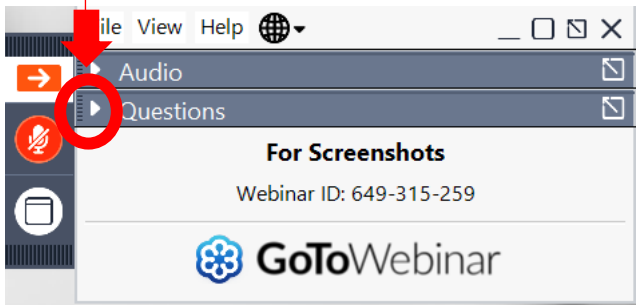
PLEASE

- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

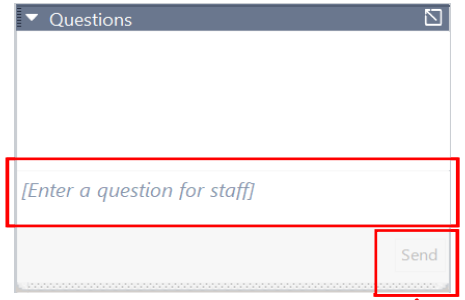
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

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.

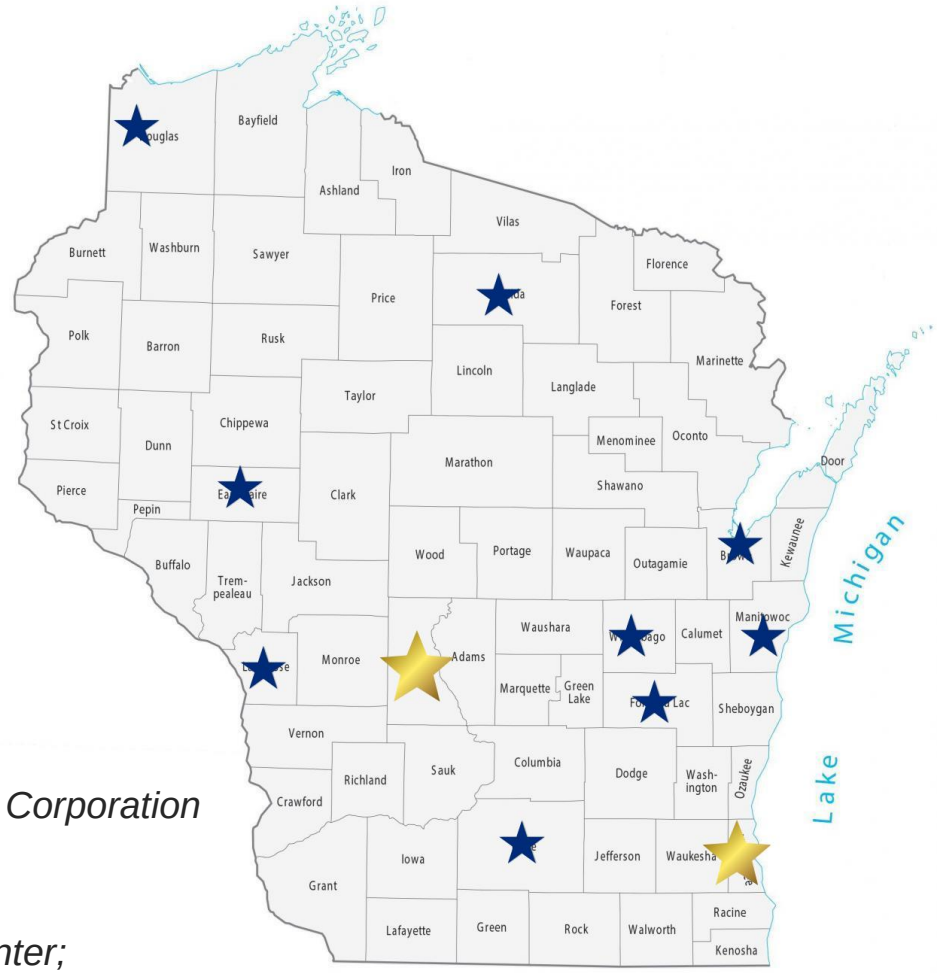
WPI provides services to all of Wisconsin's 72 counties

- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, DOD Roadmap series, Government Opportunities Business Conference, End of Year Federal Contractor Update, Annual DOD Contract Management Update, Evening FAR sessions and more……

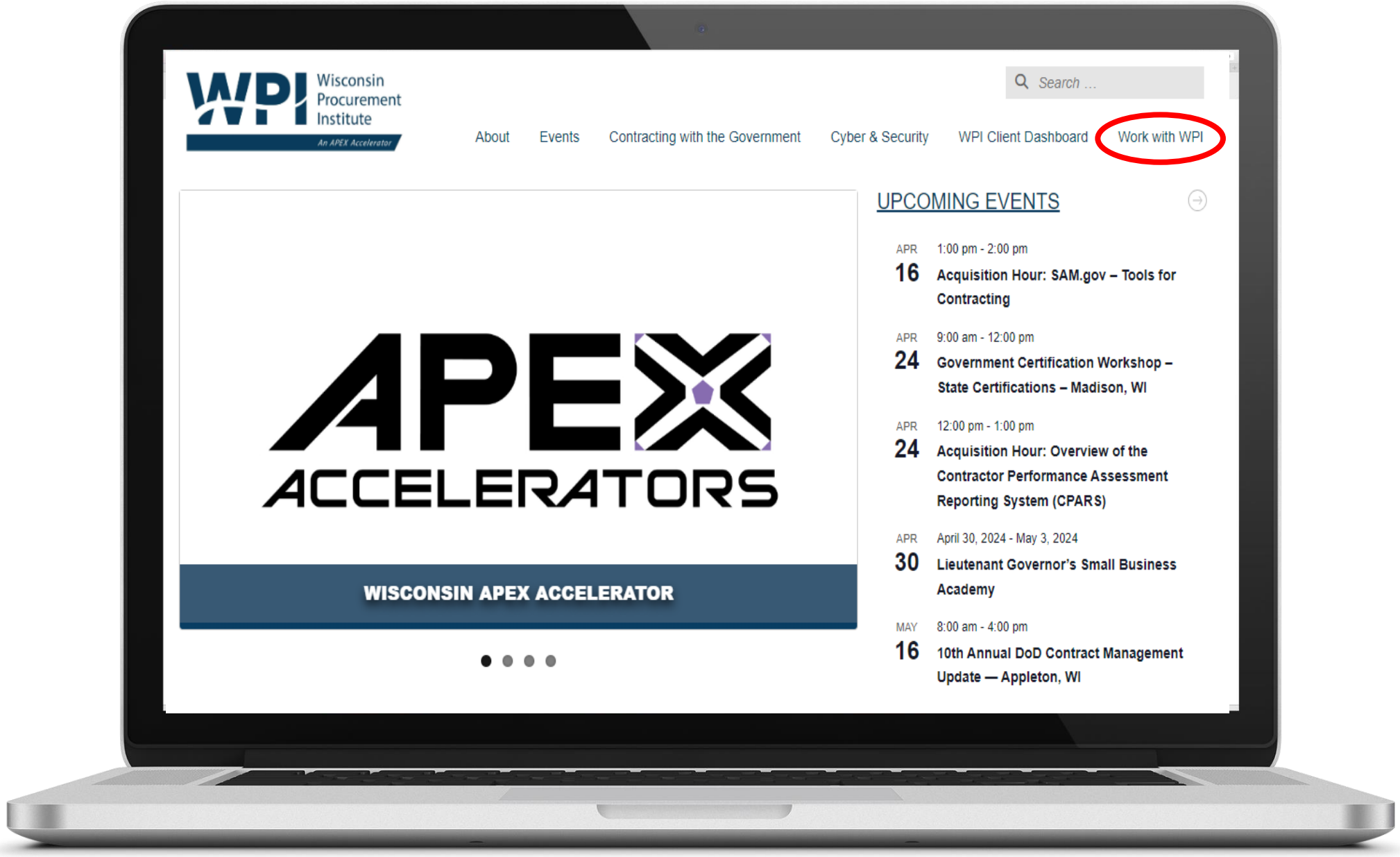
www.wispro.org

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*



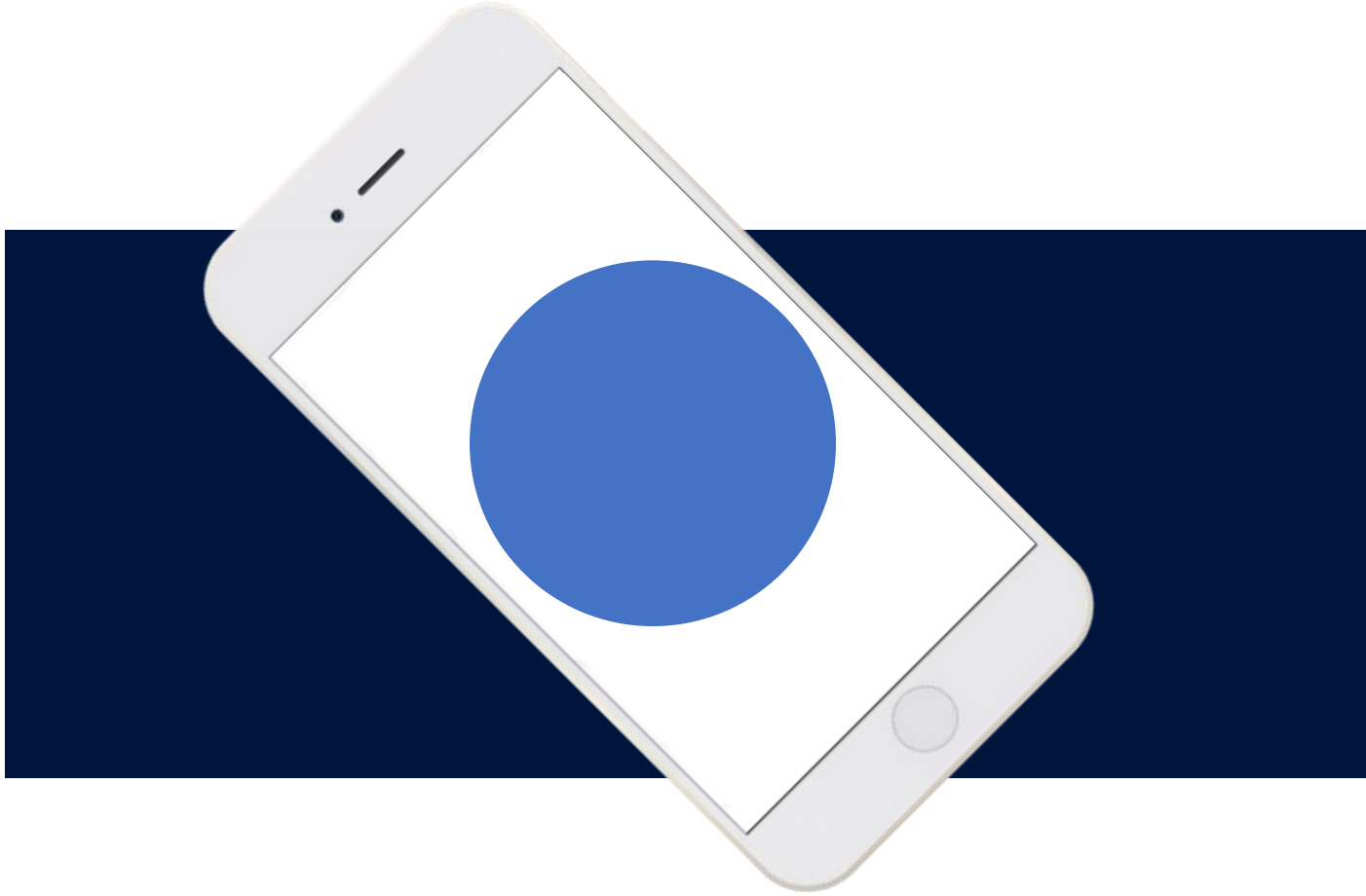
Wisconsin Procurement Institute
An APEX Accelerator


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

CMMC Update

Wisconsin Procurement Institute

AN APEX ACCELERATOR



October 25th, 2024

DFARS 252.204-7012

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.

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.

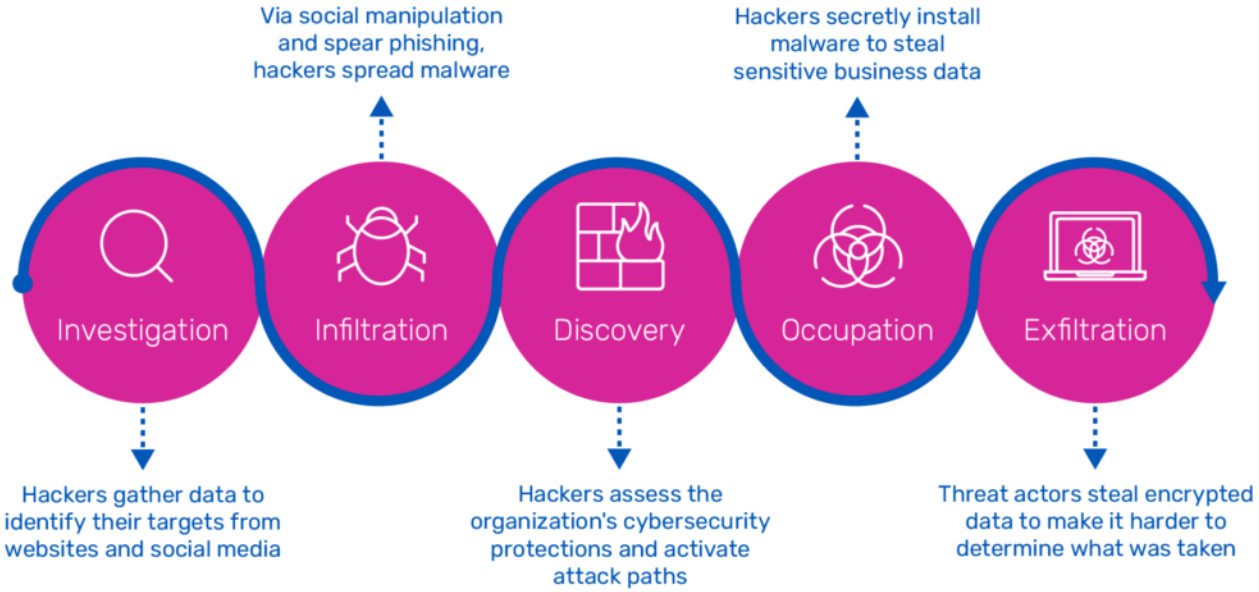
Confirmed in 2013, the theft of data from the F-35 Lightning II represented one of the most significant data breaches in world history.

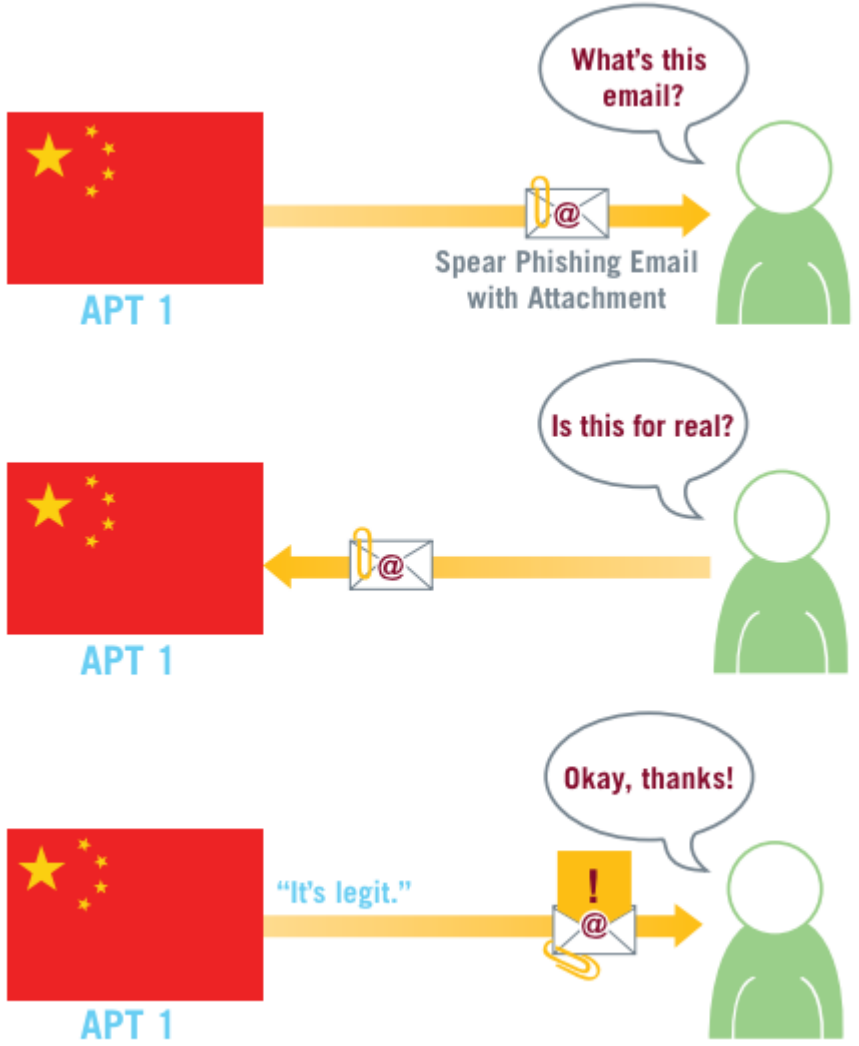
Breach involved a series of units, funded and operated by the PLA, identified as Advanced Persistent Threats (APT).

Targets were companies within Lockheed Martin's supply chain.

Data was primarily unclassified, but controlled, information.

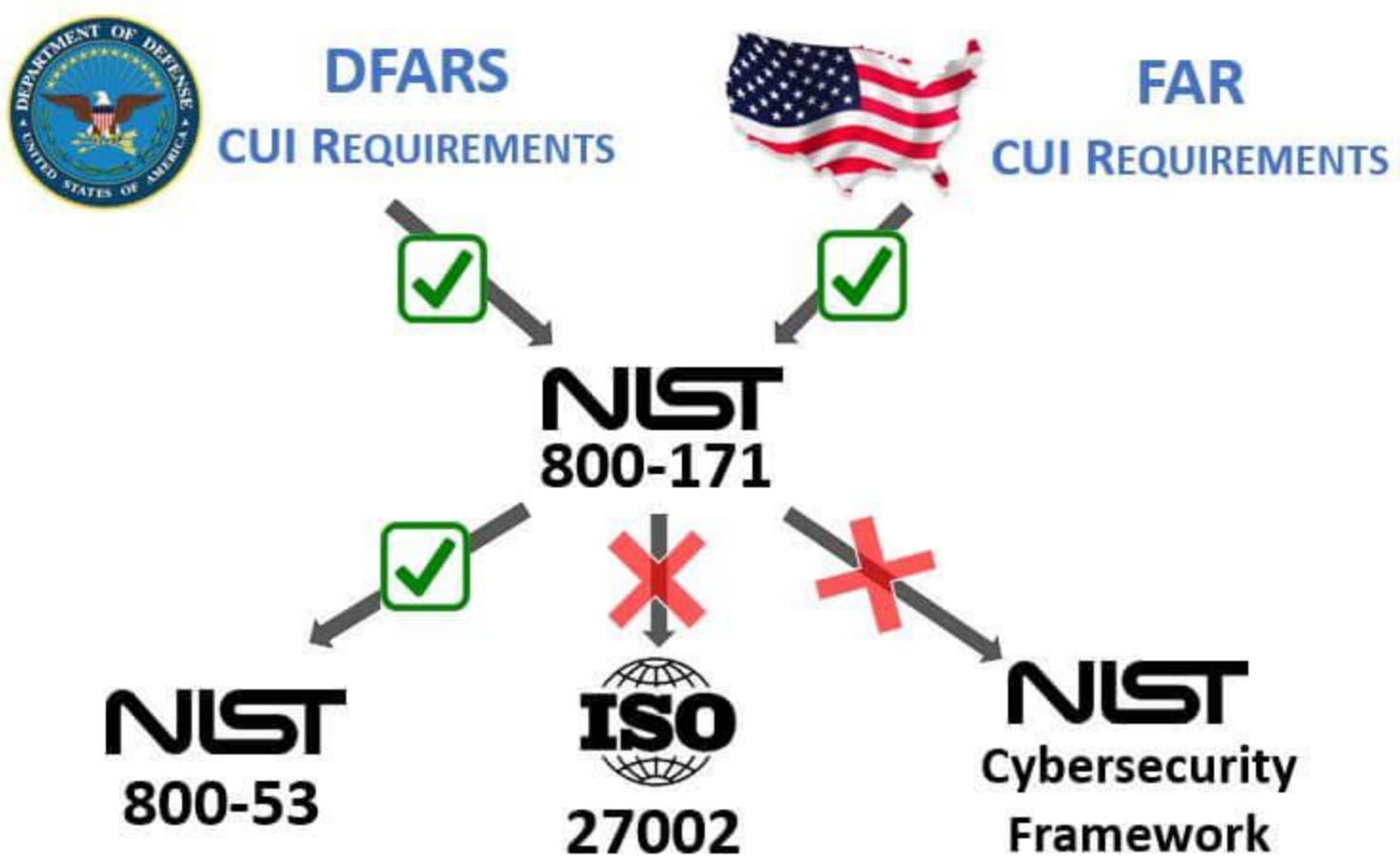
What is an Advanced Persisent Threat?






LOCKHEED MARTIN
3103

FAR 52.204-21, DFARS, NIST, and Beyond



An Evolution – Not a Departure

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

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.

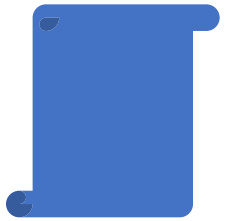
FAR 52.204-21

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.

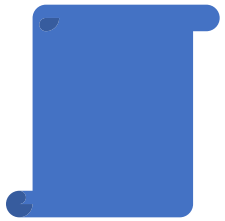
Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public.

Key Points



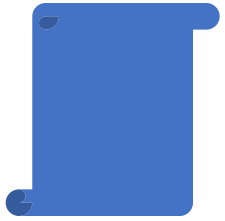
15 Controls

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



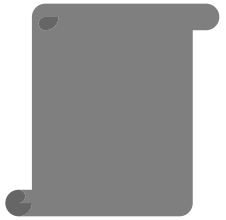
Are Echoed within NIST SP 800-171 Requirements

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**.

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

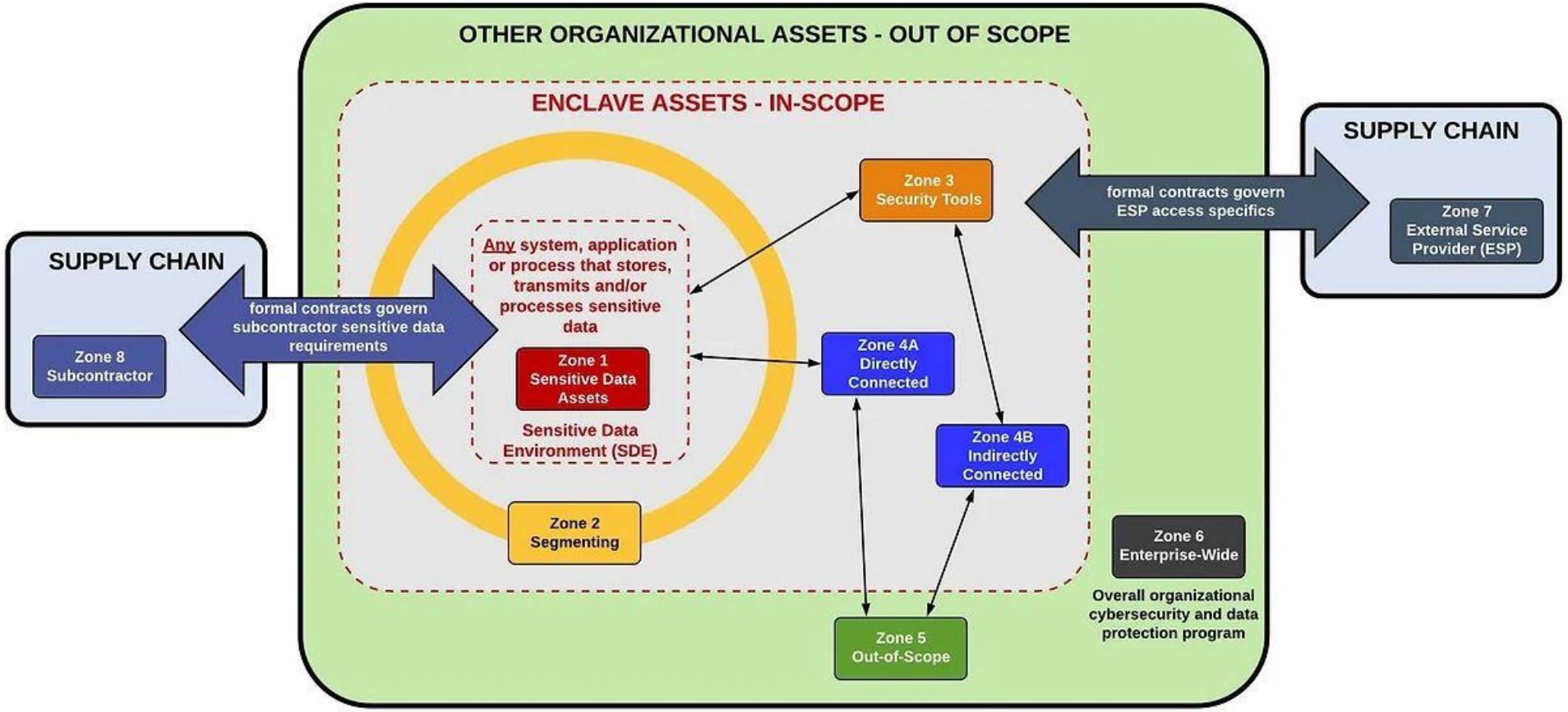
NIST
National Institute of Standards and Technology

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.

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 OBJECTIVES

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

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

ASSESSMENT METHODS

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

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

ASSESSMENT OBJECTS

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

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

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

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.

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 within five (5) business day from the Final Findings Briefing or by an alternative date determined by the Lead Assessor, but a date not to exceed five (5) calendar days prior to the submission of the Final Findings Report into CMMC eMASS.

The CMMC Final Rule was published on **October 15, 2024**. It will become effective on **Dec 16, 2024**, and enter contracts in **mid-2025** (Q2, March-April anticipated).

NIST SP 800-171r2

Chapter 3: Page 9 NIST SP 800-171r2

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

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

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

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

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

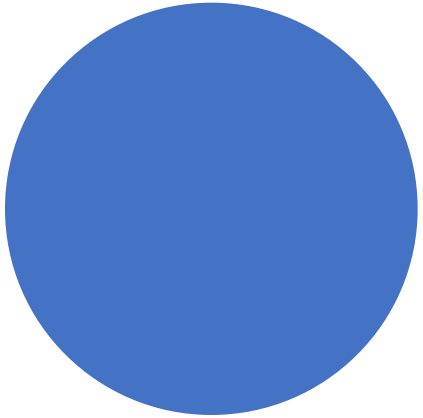
3. NIST Special Publication 800-171A
   Assessing Security Requirements for
   Controlled Unclassified Information

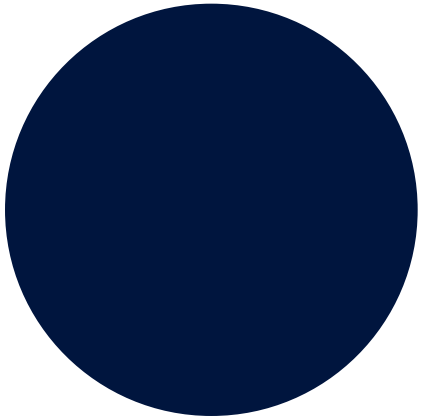
System Security Plan

- 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

Plan of Action and Milestones

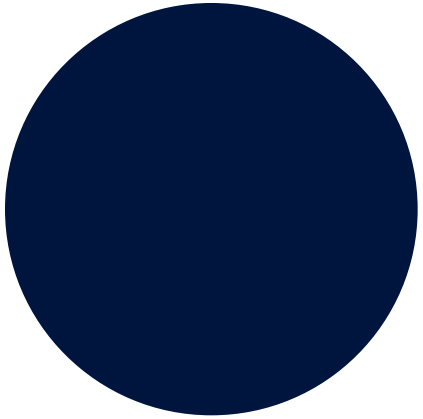
Tasks that need to be accomplished

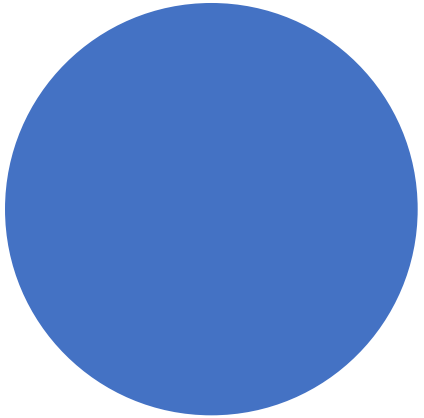




Milestones for meeting the tasks

Resources required to accomplish the elements of the plan





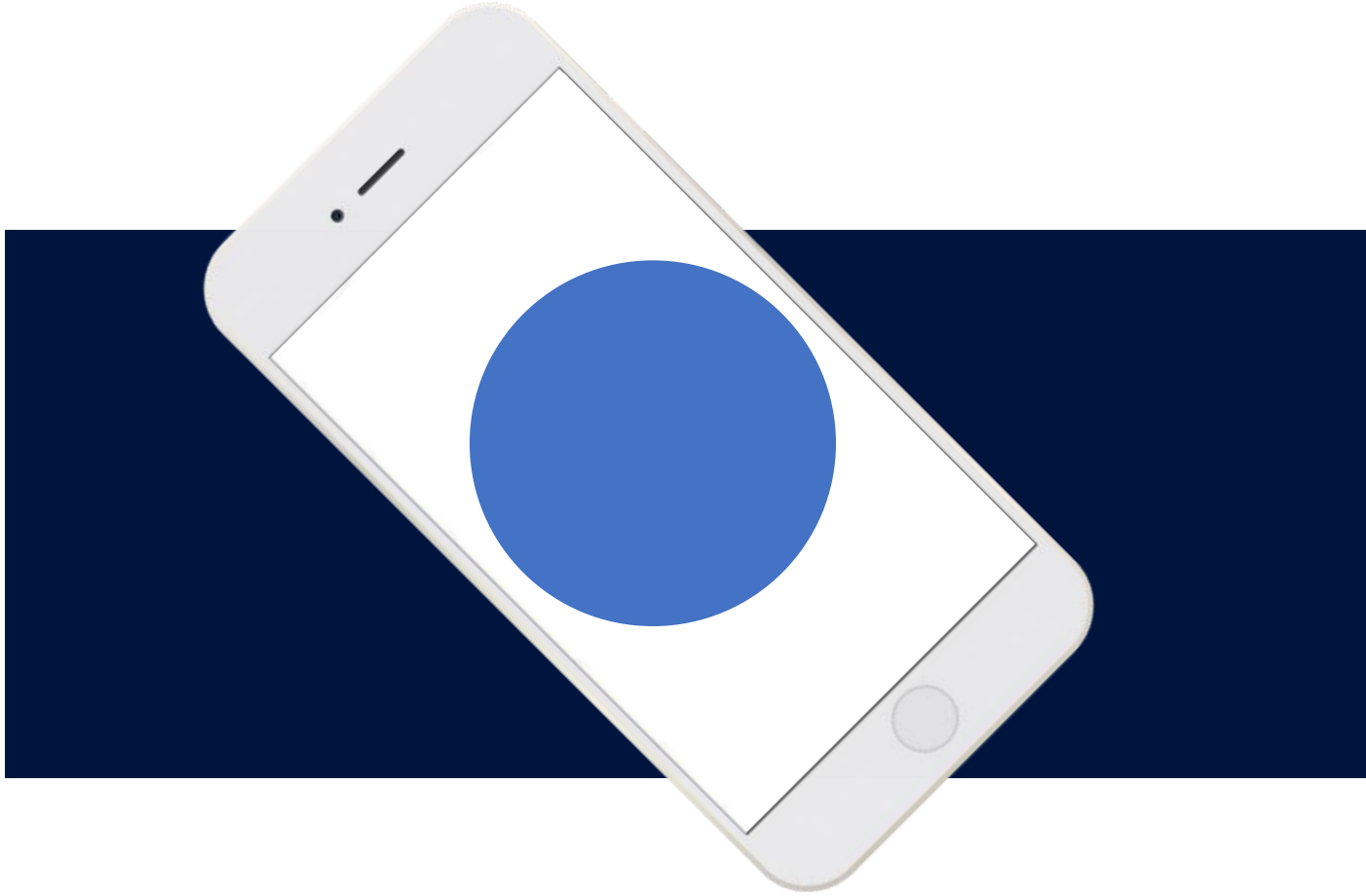
Scheduled completion dates for the milestones

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

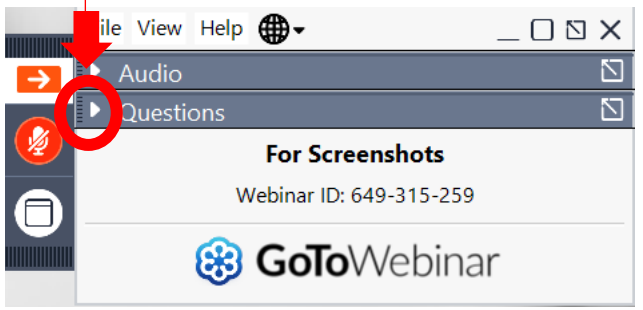
AN APEX ACCELERATOR



QUESTIONS?

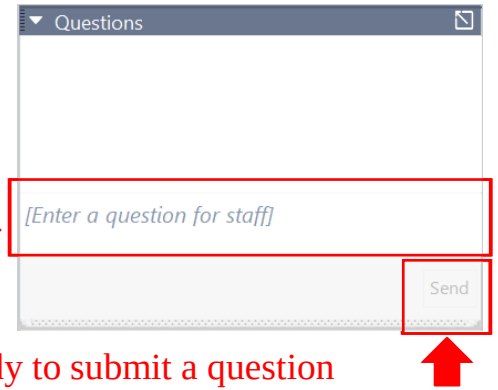
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation



Click Send when ready to submit a question

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

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 25** – CMMC Update – October 2024
- **November 12** – Preparing for One-on-One Buyer Meetings
- **November 13** – Responding to Sources Sought Notices and Preparing a Capabilities Statement
- **November 22** – CMMC Update – November 2024
- **December 20** - CMMC Update – December 2024

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

CYBER FRIDAY LIVE WEBINAR SERIES

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 18,** 3.1.7 System Maintenance Policy~~
- **November 22,** 3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security
- **January 24,** 3.1.11 Risk Assessment Policy, Security Assessment Reports

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

EMERGING ISSUES WEBINAR SERIES

This series is intended as an information tool and resource for contract managers and those with a compliance function. Attendees receive 1 CPE credit for attending.

- ~~**Oct 24 –** Innovation – What Does Innovation Look Like from DoD's Perspective?~~

- **Nov 21** – The Critical Role Your Accounting System Plays in SBIR/STTR Success

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

Expanding Business Opportunities in Rural Wisconsin

The government can be a great customer for your business – especially if you are a small business. The challenge is to know WHAT they buy, HOW they buy it, and WHEN they buy it – AND THEN – how your business can take those first steps to SUCCESSFULLY SELL to the FEDERAL GOVERNMENT. Wisconsin is home to many Federal opportunities from Ft. McCoy, US Army Corps of Engineers, National Park Service, US Forest Service and VA Hospitals and Clinics. It is also home to a number of large prime contractors including Oshkosh Defense, Wisconsin Physician Services and Michels.

November 13

Juneau County
Elroy Theatre
122 S Main St., Elroy, WI 5392

November 14

Black River Falls
Ho-Chunk Gaming (Bingo Hall)
W9010 Hwy 54E, Black River Falls, WI 54615

…More information and registrations at wispro.org/events

Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

- Save the Date -

The Contracting Academy

Developing and Growing Government Contractors

Dec 10

Virtual | 9:00 am - 4:00 pm

The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

Dec 11-12

The Baird Center

400 W Wisconsin Ave. Milwaukee WI 53203

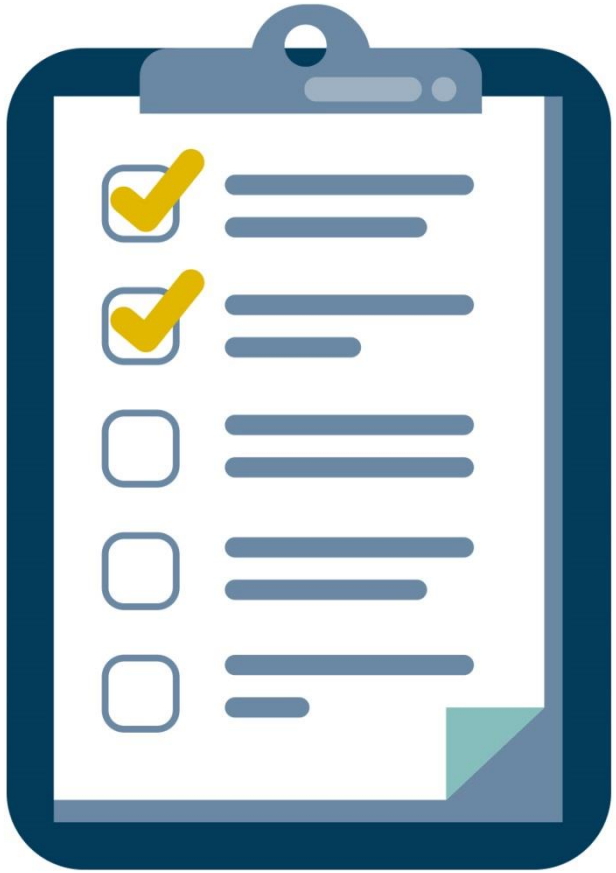
Presented by the Wisconsin Economic Development Corporation, MARKETPLACE is the Governor's Annual Conference on Diverse Business Development. This event connects business owners from across Wisconsin seeking to do business with state, federal and local governments as well as the private sector. The conference provides the opportunity for established minority-, woman-, veteran- and LGBTQ+-owned businesses and small businesses to learn from and connect with resource providers, government representatives, corporate buyers and business professionals to lay a foundation for new partnerships and business opportunities.

MarketplaceWisconsin.com

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

October 15, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Neelu Patil
neelagangap@wispro.org

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