



*An APEX Accelerator*

---

# **Acquisition Hour: Protecting Federal Contract Information (FCI): An Introduction to FAR 52.204-21**

**February 28 | 11:00 am - Noon**

**Presented by:  
Matt Frost, WPI**



# Webinar Etiquette

## PLEASE

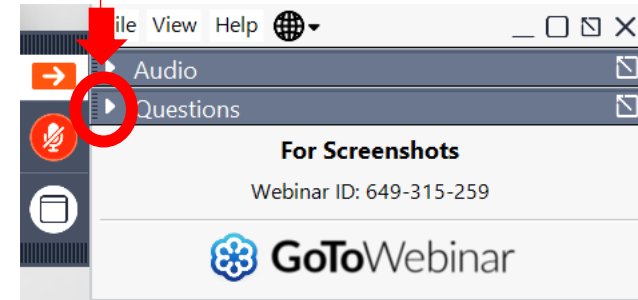
- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
  - We will share the questions with our guest speaker who will respond to the group

## THANK YOU!



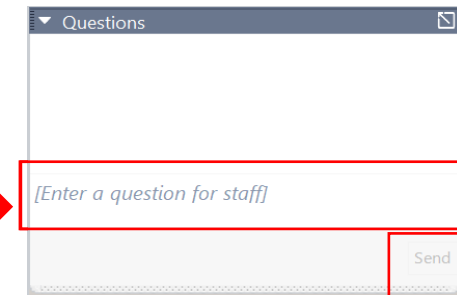
## OPENING THE QUESTIONS BOX

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





*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](http://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)*

## ▪ ASHLAND

- *Ashland Area Development Corporation*

## ▪ 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

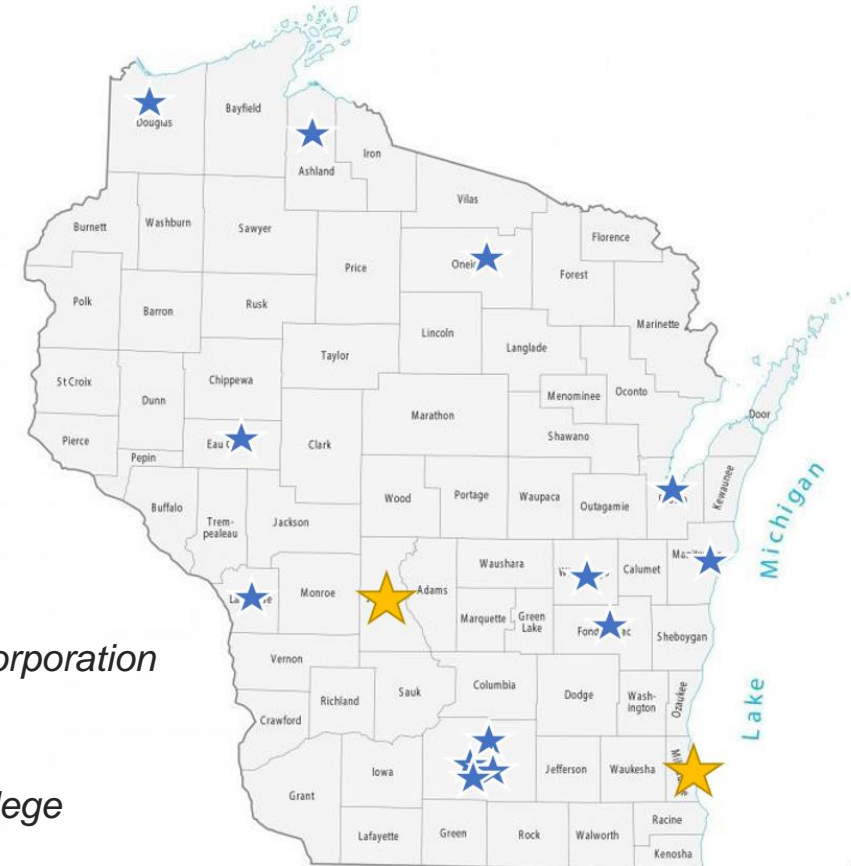
- *Greater Oshkosh Economic Development Corporation*

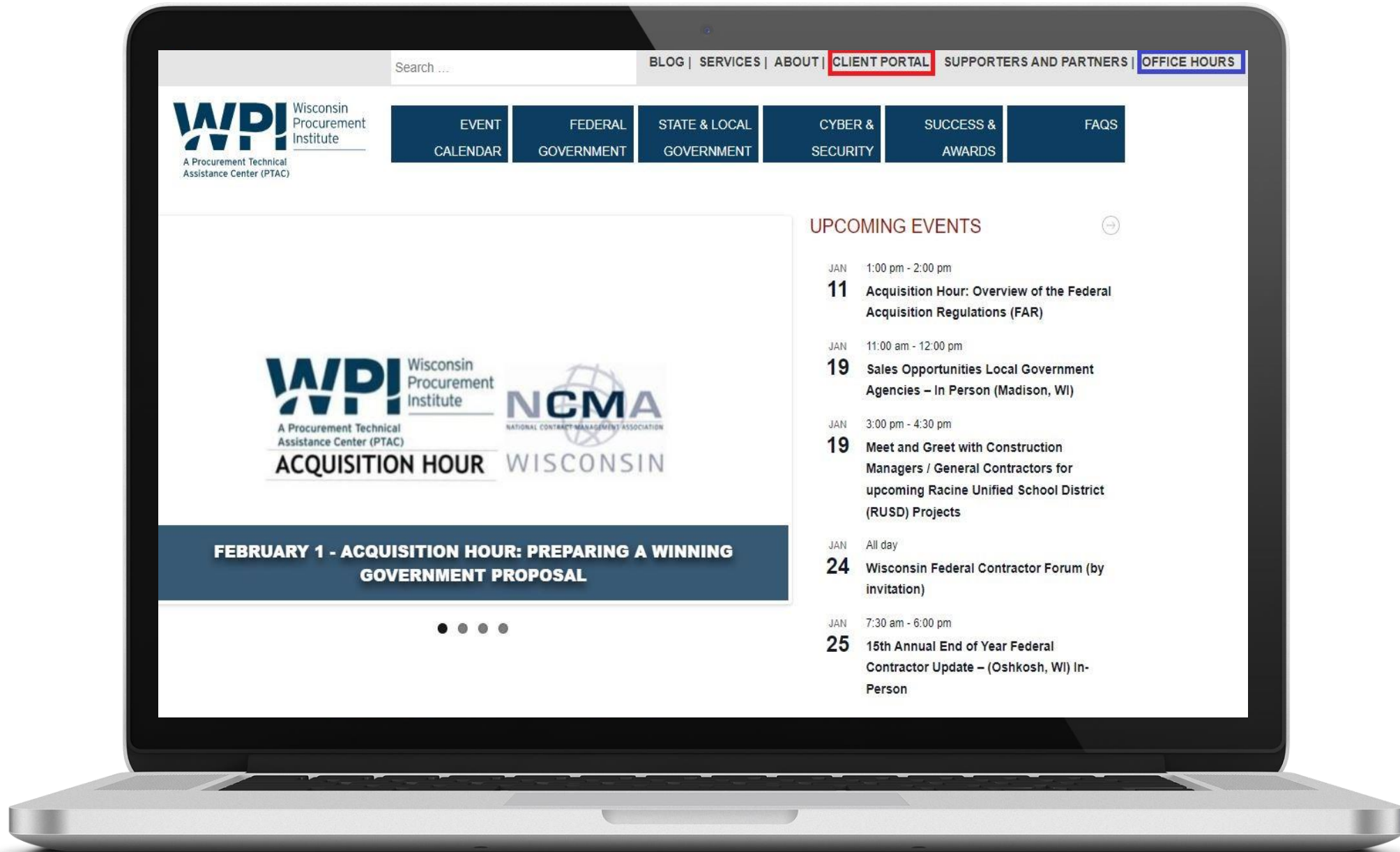
## ▪ RHINELANDER

- *Nicolet Area Technical College*

## ▪ SUPERIOR

- *Small Business Dev Center;*  
*UW Superior*





Search ...

BLOG | SERVICES | ABOUT | **CLIENT PORTAL** | SUPPORTERS AND PARTNERS | OFFICE HOURS



- EVENT CALENDAR
- FEDERAL GOVERNMENT
- STATE & LOCAL GOVERNMENT
- CYBER & SECURITY
- SUCCESS & AWARDS
- FAQS



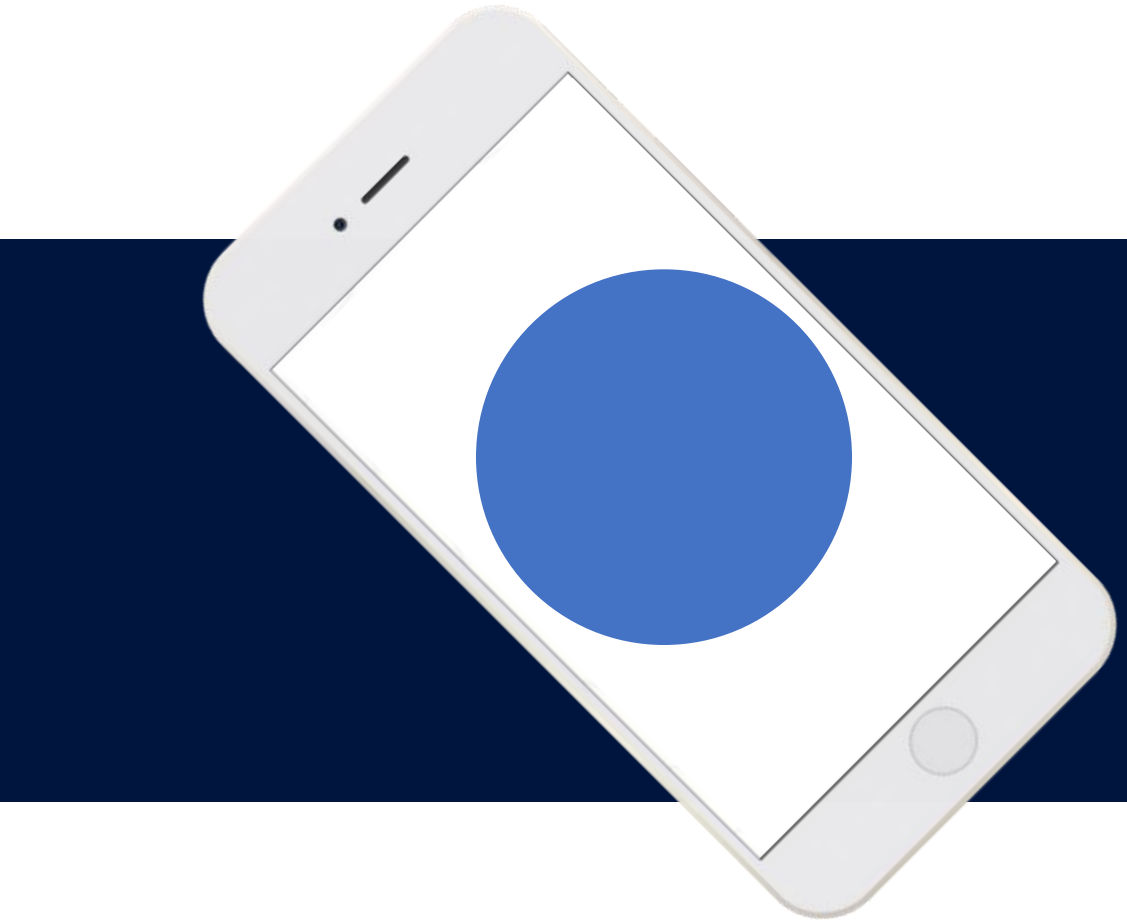
**FEBRUARY 1 - ACQUISITION HOUR: PREPARING A WINNING GOVERNMENT PROPOSAL**



### UPCOMING EVENTS



- JAN 1:00 pm - 2:00 pm  
**11** Acquisition Hour: Overview of the Federal Acquisition Regulations (FAR)
- JAN 11:00 am - 12:00 pm  
**19** Sales Opportunities Local Government Agencies – In Person (Madison, WI)
- JAN 3:00 pm - 4:30 pm  
**19** Meet and Greet with Construction Managers / General Contractors for upcoming Racine Unified School District (RUSD) Projects
- JAN All day  
**24** Wisconsin Federal Contractor Forum (by invitation)
- JAN 7:30 am - 6:00 pm  
**25** 15th Annual End of Year Federal Contractor Update – (Oshkosh, WI) In-Person



February 14th, 2024



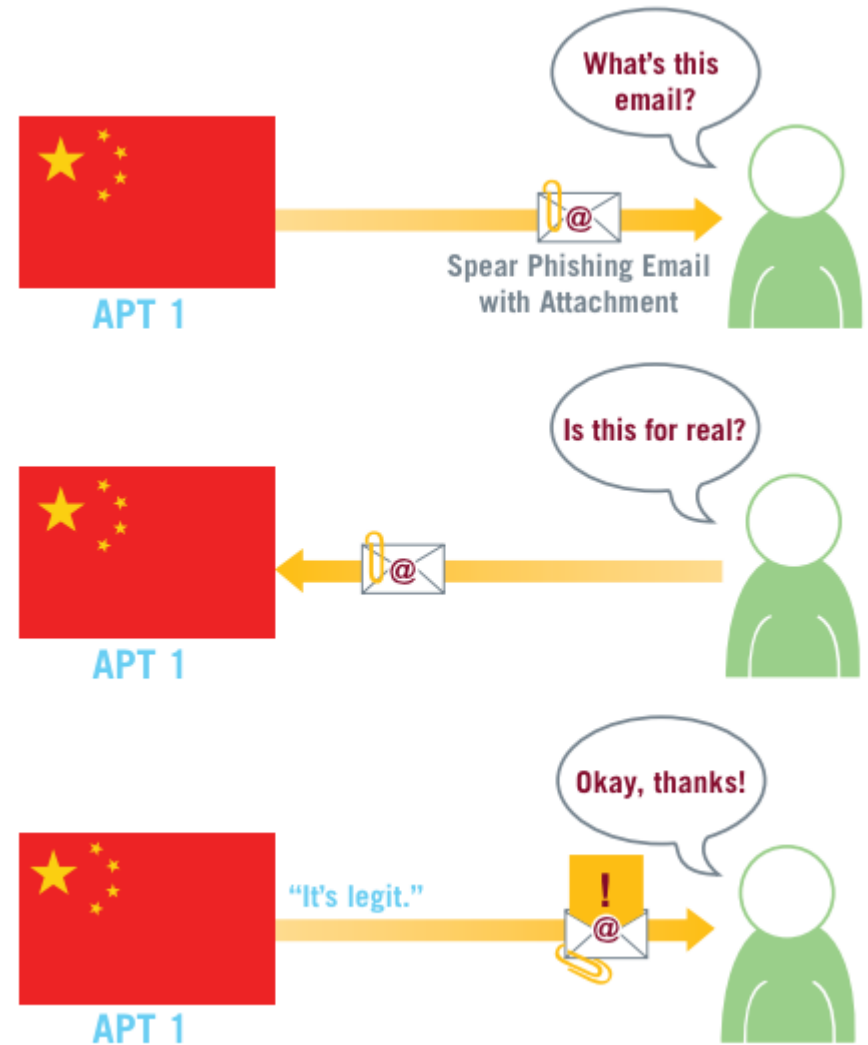
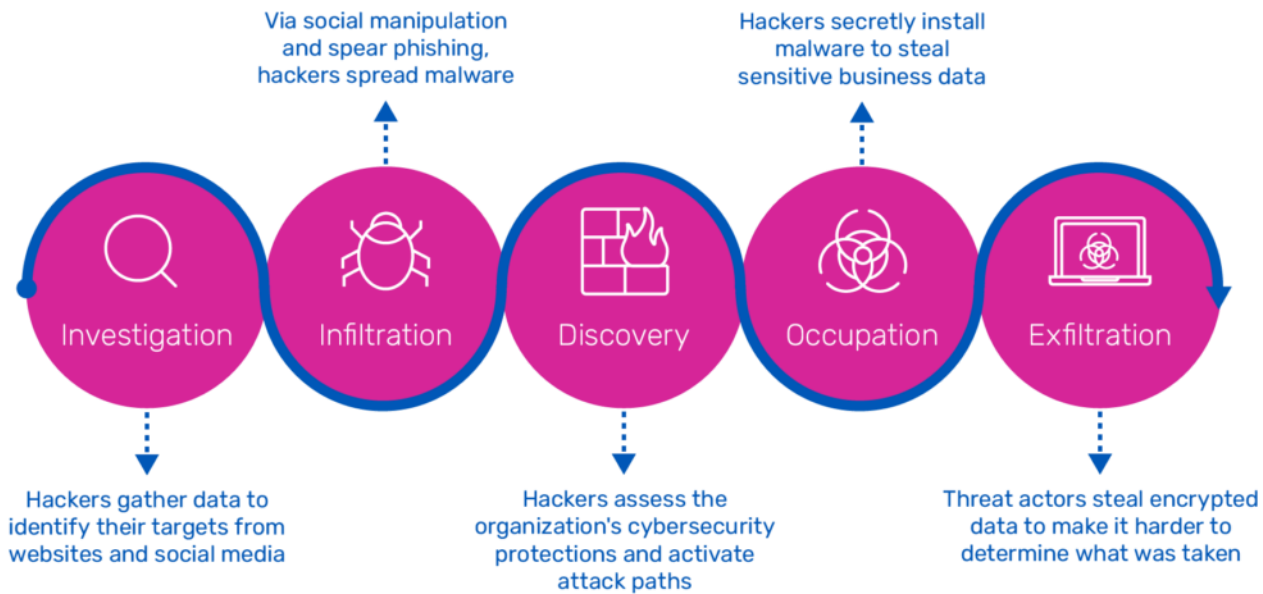
Confirmed in 2013, the theft of data from the F-35 Lightning II represented one of the largest data breaches in world history.

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?





1



FAR 52.204-21

2



What is FCI?

3



Requirements for  
Completion





## 52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

---

1

The FAR

<https://www.acquisition.gov/far/52.204-21>

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

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

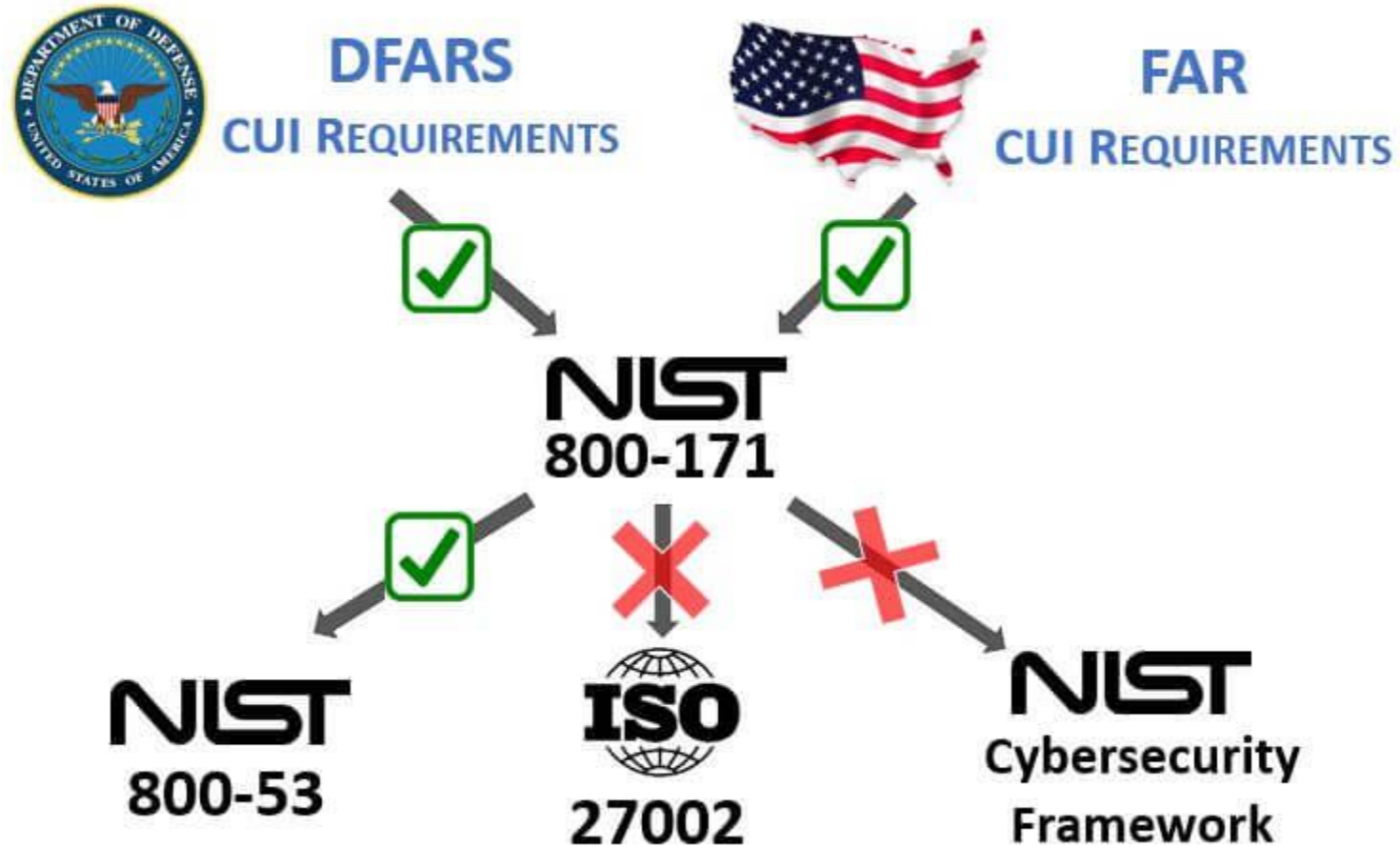
Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

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.

# 15 Controls

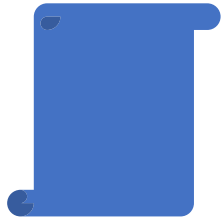
- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

# FAR 52.204-21, DFARS, NIST, and Beyond



An Evolution – Not a Departure

# Key Points



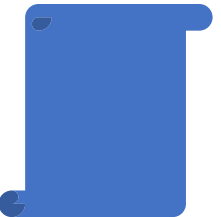
## **15 Controls**

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



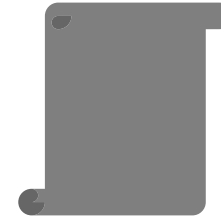
## **Are Echoed within NIST SP 800-171 Requirements**

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.

1



FAR 52.204-21

2



What is FCI?

3



Requirements for Compliance



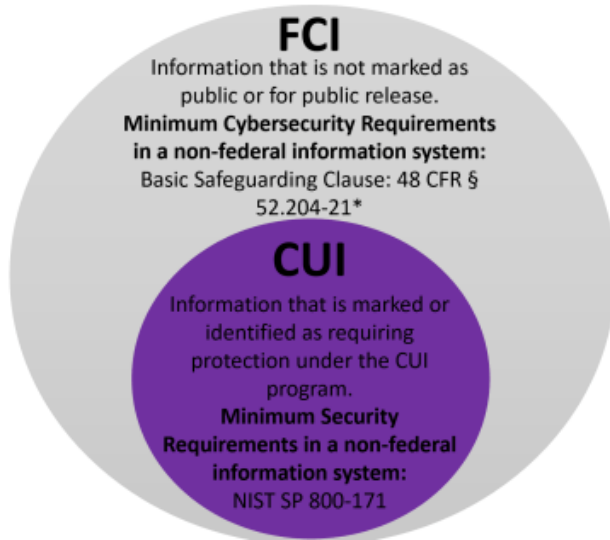
## What is FCI?

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.

## Paragraph C

The Contractor **shall** include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, **other than commercially available off-the-shelf items**), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

**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

1



FAR 52.204-21

2



What is FCI?

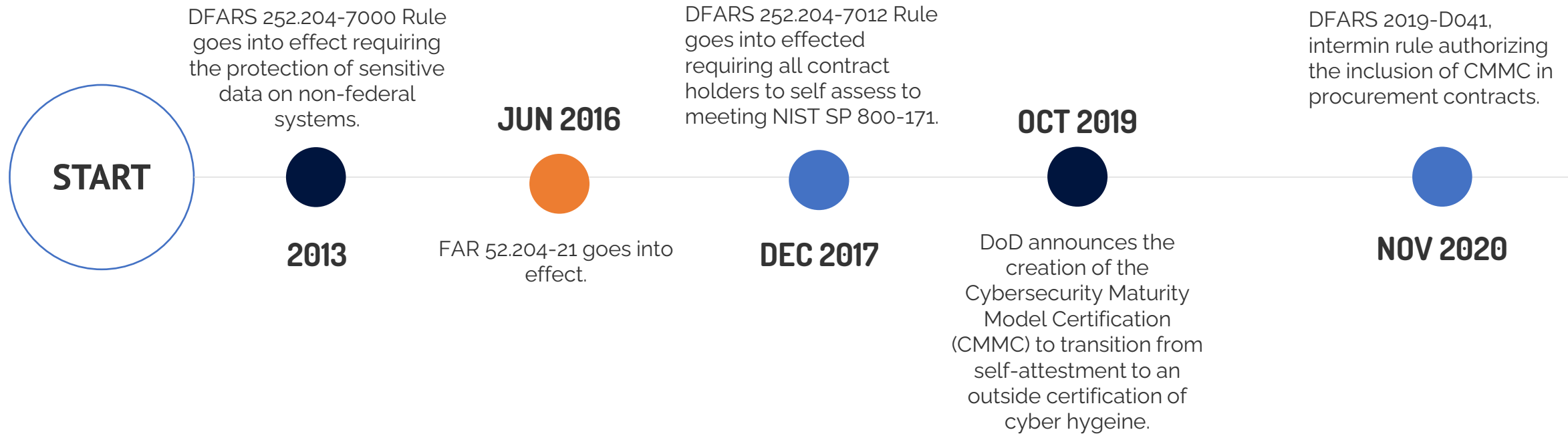
3



Requirements for Compliance



# Cybersecurity Timeline



# Cybersecurity Timeline

**DEC 8 2020**



DOD and Cyber (Formerly CMMC)-AB release an updated timeline – stating the model has to be fully implemented by September 2021.

General Services Administration acknowledges that while CMMC only applies currently to DOD contracts – ALL government contractors civilian or military should prepare to meet CMMC.



**DEC 31 2020**

**NOV 4 2021**



DOD announces release of CMMC 2.0 – streamlining the additional requirements.

CMMC Proposed Rule



**NOV 2023**



**Spring  
2025?**

# Build a Program

#	FAR 52.204-21 Cybersecurity Requirement	Control Type			Documentation Expectation		
		Technical	Administrative	Physical	Policies	Standards	Procedures
52.204-21(b)	Safeguarding requirements and procedures.	X	X	X	X	X	X
52.204-21(b)(1)	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:		X		X	X	X
52.204-21(b)(1)(i)	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	X			X	X	X
52.204-21(b)(1)(ii)	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	X			X	X	X
52.204-21(b)(1)(iii)	Verify and control/limit connections to and use of external information systems.	X	X		X	X	X
52.204-21(b)(1)(iv)	Control information posted or processed on publicly accessible information systems.		X		X	X	X
52.204-21(b)(1)(v)	Identify information system users, processes acting on behalf of users, or devices.	X	X		X	X	X
52.204-21(b)(1)(vi)	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	X			X	X	X
52.204-21(b)(1)(vii)	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.		X	X	X	X	X
52.204-21(b)(1)(viii)	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.			X	X	X	X
52.204-21(b)(1)(ix)	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.		X	X	X	X	X
52.204-21(b)(1)(x)	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	X	X		X	X	X
52.204-21(b)(1)(xi)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	X			X	X	X
52.204-21(b)(1)(xii)	Identify, report, and correct information and information system flaws in a timely manner.	X	X		X	X	X
52.204-21(b)(1)(xiii)	Provide protection from malicious code at appropriate locations within organizational information systems.	X			X	X	X
52.204-21(b)(1)(xiv)	Update malicious code protection mechanisms when new releases are available.	X			X	X	X
52.204-21(b)(1)(xv)	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	X			X	X	X
52.204-21(b)(2)	Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.		X		X	X	X
52.204-21(c)	Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.		X		X	X	X

### AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

---

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

### ASSESSMENT OBJECTIVES [NIST SP 800-171A]

---

Determine if:

- [a] authorized users are identified;
- [b] processes acting on behalf of authorized users are identified;
- [c] devices (and other systems) authorized to connect to the system are identified;
- [d] system access is limited to authorized users;
- [e] system access is limited to processes acting on behalf of authorized users; and
- [f] system access is limited to authorized devices (including other systems).



1



## FOUNDATIONAL

An organization must demonstrate basic cyber hygiene practices, such as ensuring employees change passwords regularly to protect Federal Contract Information (FCI). FCI is "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."

2



## ADVANCED

An organization must have an institutionalized management plan to implement good cyber hygiene practices to safeguard CUI, including all the NIST 800-171 r2 security requirements and processes.

3



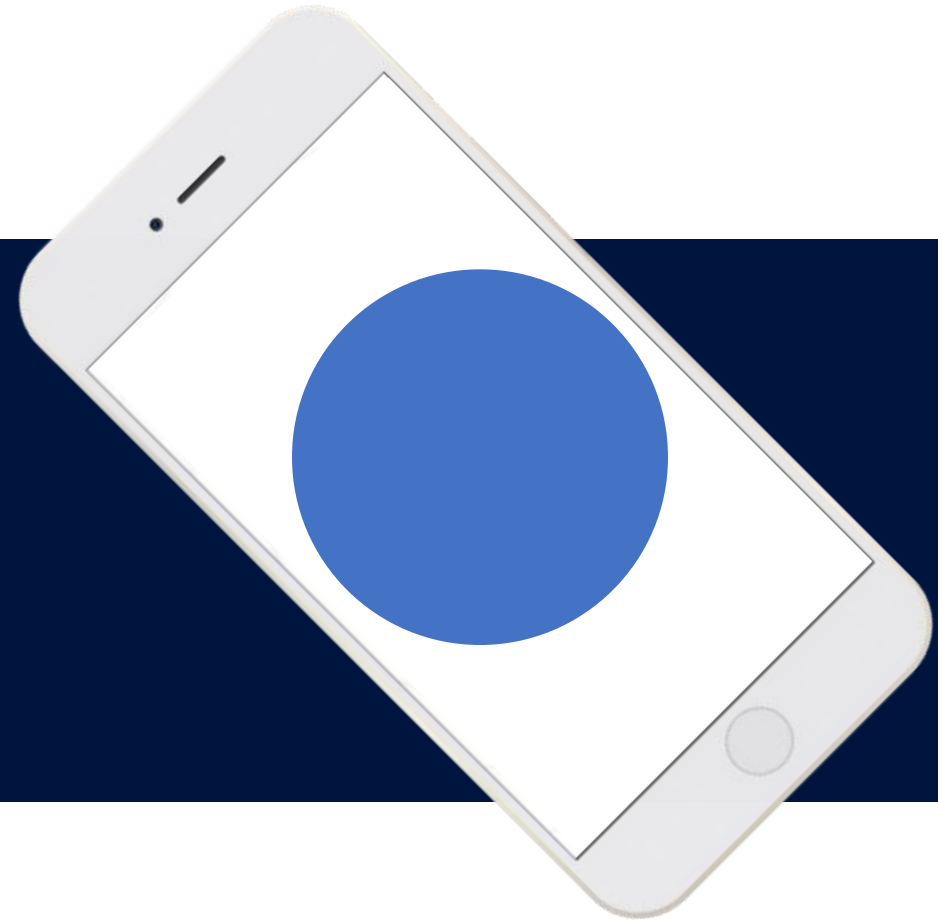
## EXPERT

An organization must have standardized and optimized processes in place and additional enhanced practices that detect and respond to changing tactics, techniques and procedures (TTPs) of advanced persistent threats (APTs). An APT is as an adversary that possesses sophisticated levels of cyber expertise and significant resources to conduct attacks from multiple vectors. Capabilities include having resources to monitor, scan, and process data forensics..



Wisconsin  
Procurement  
Institute

**APEX**  
ACCELERATORS



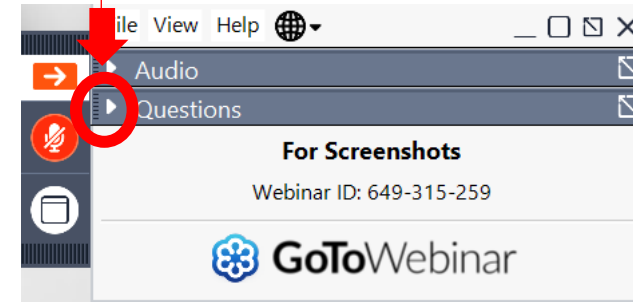
**APEX**  
ACCELERATORS

# QUESTIONS?



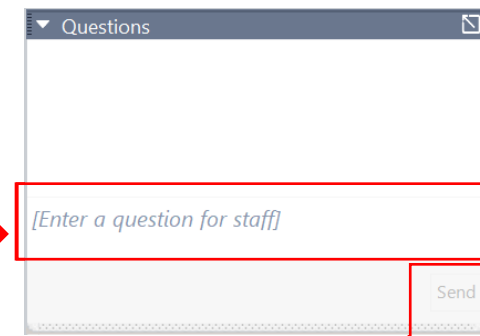
## OPENING THE QUESTIONS BOX

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

- February 28  
**Protecting Federal Contract Information (FCI): An Introduction to FAR 52.204-21**
- March 12  
**U.S. SBA Surety Bond Guarantees: What to Know**
- March 27  
**Preparing a Winning Government Proposal**

**...More information and registrations at [wispro.org/events](https://wispro.org/events)**

# EMERGING ISSUES LIVE WEBINAR SERIES

- February 29  
**From SBIR/STTR to DPA Title III – An Overview of Federal Innovation Programs, Needs and Marketplace**
- March 14  
**Suggested Process for Creating a Federal Business Development Strategy**
- March 28  
**Defense Production Act Title III – Unique Opportunities for Unique Companies**

**...More information and registrations at [wispro.org/events](http://wispro.org/events)**

*Registration Now Open*



---

# **Announcing 2024 Evening FAR Sessions**

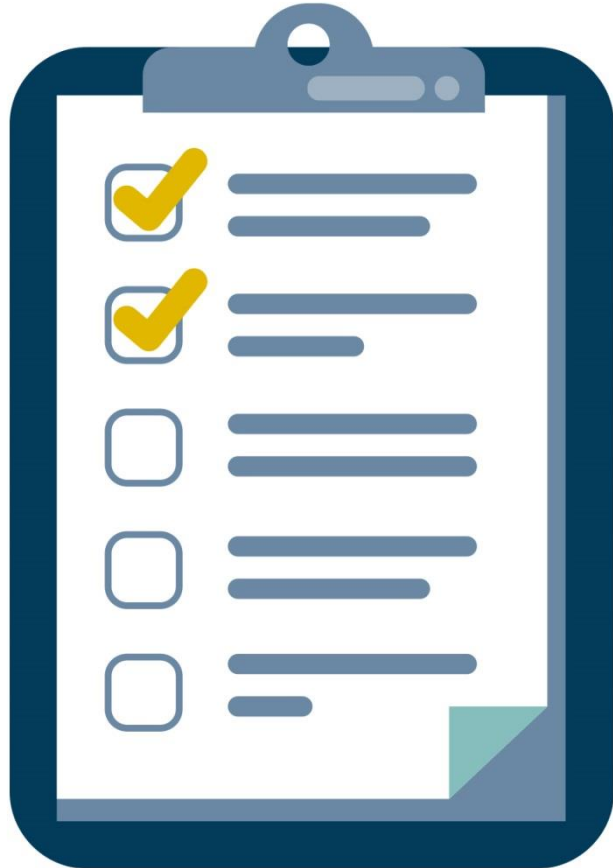
*January 30 – March 19*

---

*[Wispro.org/Events](https://wispro.org/events)*

February 28, 2024

# SURVEY



February 28, 2024

# CONTINUING PROFESSIONAL EDUCATION



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

**Neelu Patil**

[neelagangap@wispro.org](mailto:neelagangap@wispro.org)

# PRESENTED BY

Wisconsin Procurement Institute (WPI)

[www.wispro.org](http://www.wispro.org)

# Matt Frost

Wisconsin Procurement Institute

mattf@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320  
Milwaukee WI 53226