Wisconsin Procurement Institute
AN APEX ACCELERATOR

APEX ACCELERATORS

Cyber Friday:
NIST SP 800.171 – 3.2 – Awareness & Training and 3.3 Audit & Accountability

September 15 | 11:00 am – Noon
Presented by Matt Frost, WPI

Wisconsin Procurement Institute
Cyber Friday

Webinar Etiquette

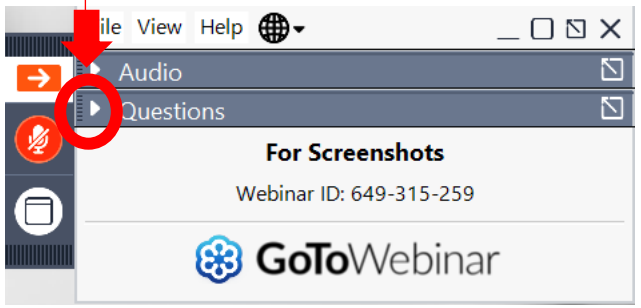
PLEASE

- § 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!

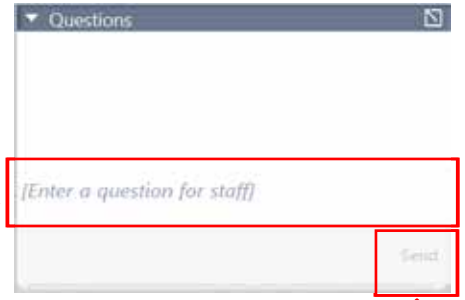
OPENING THE QUESTIONS BOX

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

WPI is Wisconsin's APEX ACCLERATOR

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.

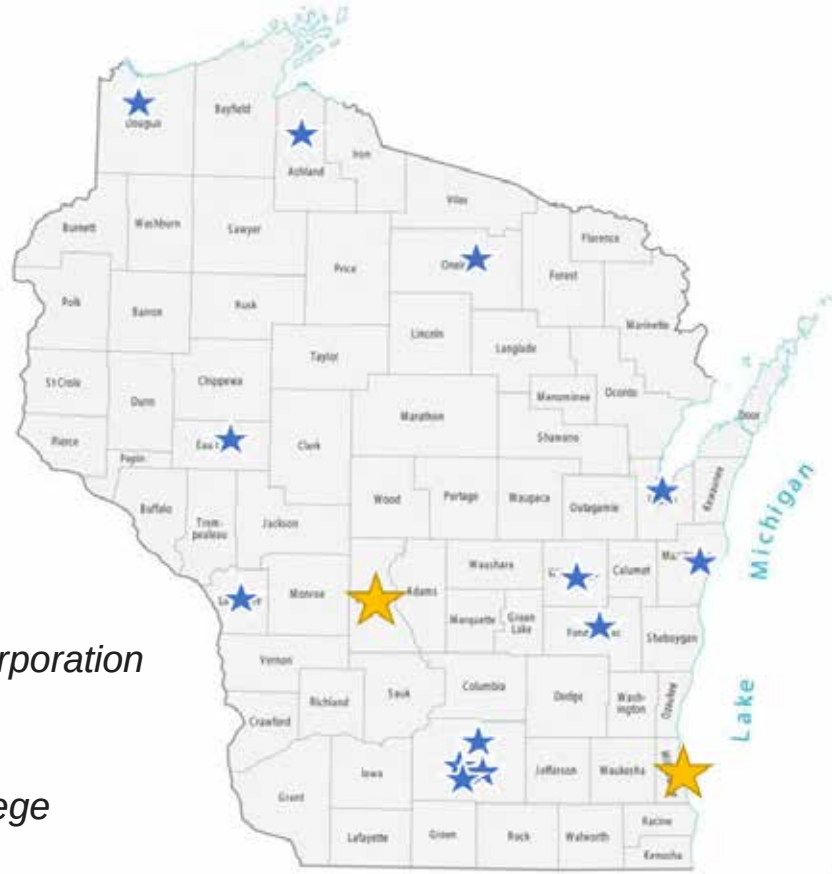
WPI provides services to all of Wisconsin's 72 counties

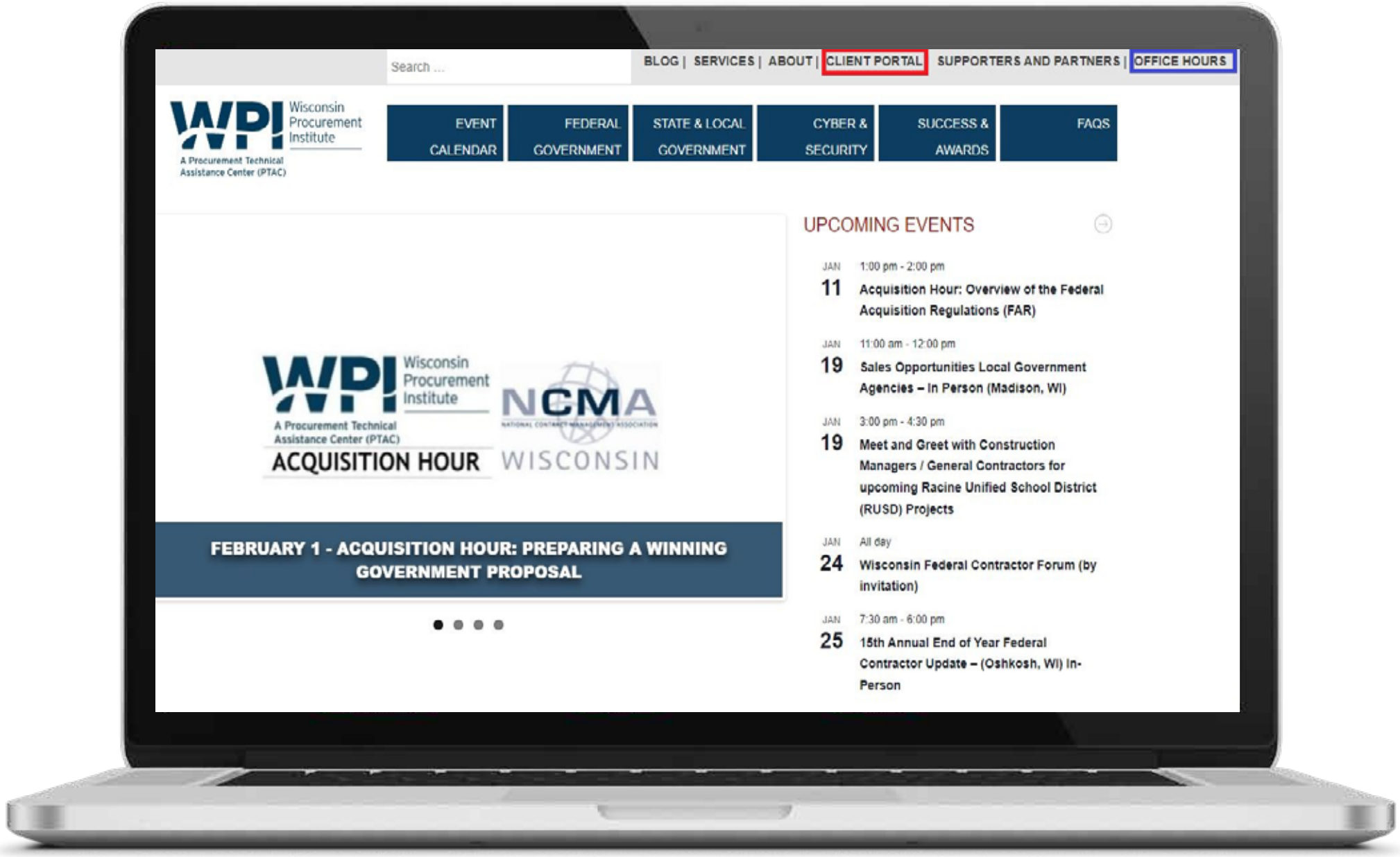
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays, 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)*
- **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*

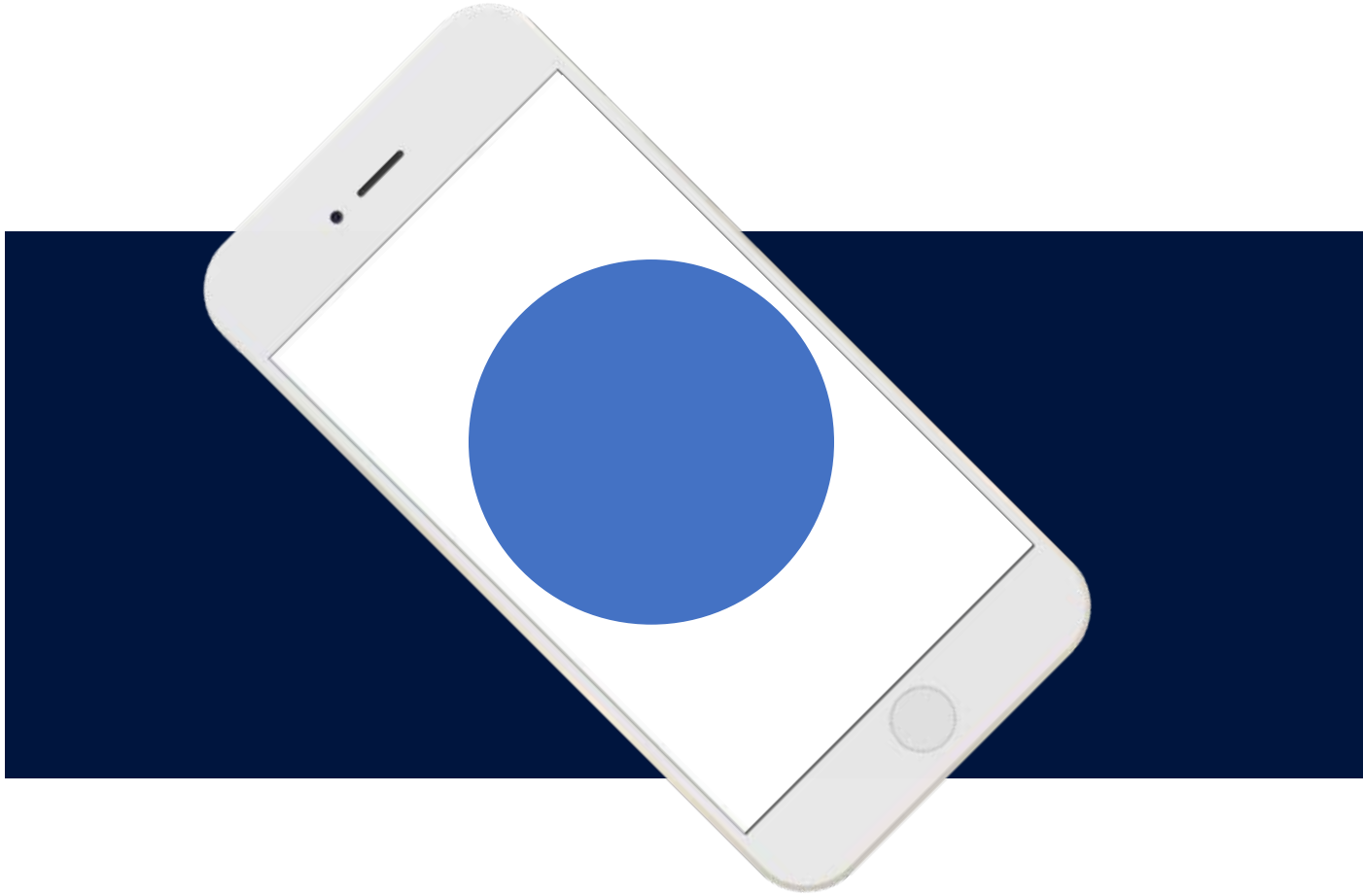



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL | SUPPORTERS AND PARTNERS | OFFICE HOURS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR
NCMA WISCONSIN
FEBRUARY 1 - ACQUISITION HOUR: PREPARING A WINNING GOVERNMENT PROPOSAL
UPCOMING EVENTS
JAN 11 1:00 pm - 2:00 pm
Acquisition Hour: Overview of the Federal Acquisition Regulations (FAR)
JAN 19 11:00 am - 12:00 pm
Sales Opportunities Local Government Agencies – In Person (Madison, WI)
JAN 19 3:00 pm - 4:30 pm
Meet and Greet with Construction Managers / General Contractors for upcoming Racine Unified School District (RUSD) Projects
JAN 24 All day
Wisconsin Federal Contractor Forum (by invitation)
JAN 25 7:30 am - 6:00 pm
15th Annual End of Year Federal Contractor Update – (Oshkosh, WI) In-Person

Introduction to NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – September 15th, 2023

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.

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.

14 Families – 110 Controls – 320 Audit Objectives

- Access Control
- **Awareness and Training**
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communications Protection
- System and Information Integrity

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. NIST SP 800-181r2 — NIST Special Publication 800-171 Revision 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Reading the Controls

NIST SP 800-171

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

3.2.1 **Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.**

DISCUSSION

Organizations determine the content and frequency of security awareness training and security awareness techniques based on the specific organizational requirements and the systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security. Security awareness techniques include: formal training; offering supplies inscribed with security reminders; generating email advisories or notices from organizational officials; displaying logon screen messages; displaying security awareness posters; and conducting information security awareness events.

3.2.1	**SECURITY REQUIREMENT** Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.1[a] *security risks associated with organizational activities involving CUI are identified.*
	3.2.1[b] *policies, standards, and procedures related to the security of the system are identified.*
	3.2.1[c] *managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.*
	3.2.1[d] *managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training]. **Test**: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].

3.2 Awareness & Training

Periodic

Build Culture

Documented

Role-Based

Controls & Objectives

NIST SP 800-171

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

Training Intentions

Security Awareness Training

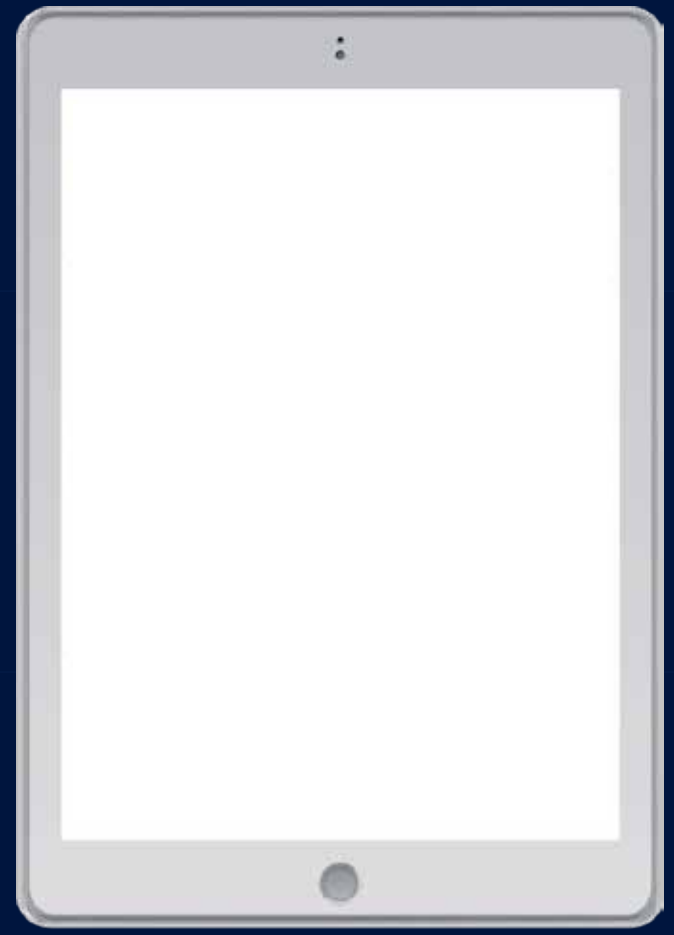
- Threat Environment
- Information Classification
- See Something / Say Something
- Good Cyber Behaviors

Role-Based Security Training

- Responsibilities
- Who To Notify
- Periodic and Accurate

Insider Threats

- Disgruntled Employees
- Intruders and/ or Vendors
- Disengaged and/ or Untrained Personnel



Security Awareness

3.2.1	**SECURITY REQUIREMENT** Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.2.1[a]	*security risks associated with organizational activities involving CUI are identified.*
	3.2.1[b]	*policies, standards, and procedures related to the security of the system are identified.*
	3.2.1[c]	*managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.*
	3.2.1[d]	*managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; relevant codes of federal regulations; security awareness training curriculum; security awareness training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for security awareness training; personnel with information security responsibilities; personnel composing the general system user community; personnel with responsibilities for role-based awareness training]. **Test**: [*SELECT FROM:* Mechanisms managing security awareness training; mechanisms managing role-based security training].	

3.2.1– Meeting the Controls

THREAT ENVIRONMENT

INCIDENT EXAMPLES

CUI EXPLANATIONS

3.2.1[a] security risks associated with organizational activities involving CUI are identified.

3.2.1[c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.

SECURITY AWARENESS AND TRAINING POLICY

INCIDENT RESPONSE POLICY

ACCEPTABLE USE POLICY

3.2.1[b] policies, standards, and procedures related to the security of the system are identified.

3.2.1[c] managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

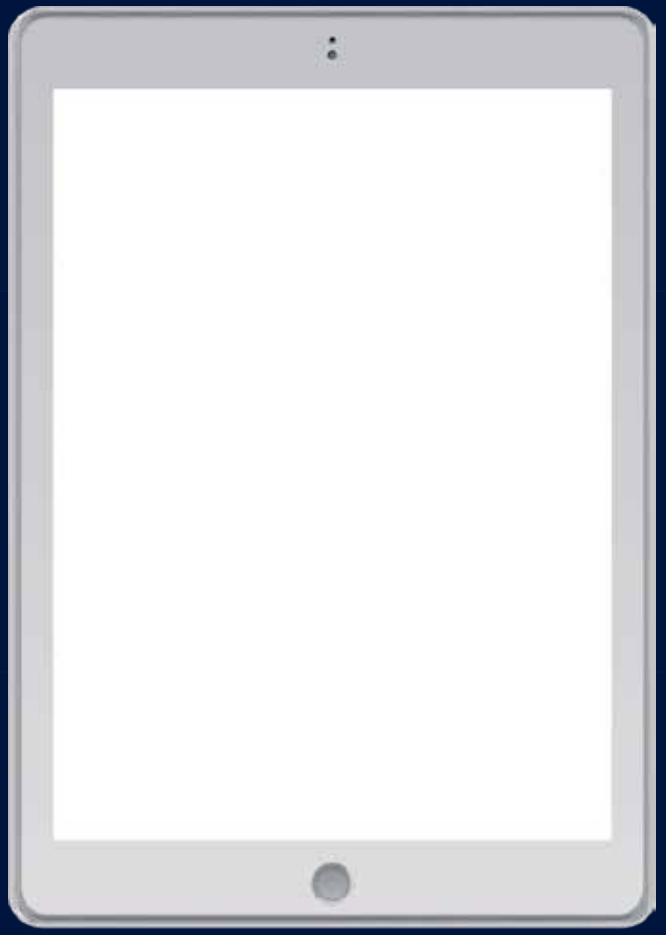
Role-Based Trainings

3.2.2	**SECURITY REQUIREMENT** Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.2.2[a]	*information security-related duties, roles, and responsibilities are defined.*
	3.2.2[b]	*information security-related duties, roles, and responsibilities are assigned to designated personnel.*
	3.2.2[c]	*personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; system security plan; training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for role-based security training; personnel with assigned system security roles and responsibilities; personnel with responsibilities	

3.2.2 – Meeting the Controls

ESTABLISHED SECURITY ROLES RESPONSIBILITY MATRIX	3.2.2[a] information security-related duties, roles, and responsibilities are defined. 3.2.2[b] information security-related duties, roles, and responsibilities are assigned to designated personnel.
INCIDENT RESPONSE POLICY SECURITY AWARENESS AND TRAINING	3.2.2[c] personnel are adequately trained to carry out their assigned information security-related duties, roles, and responsibilities.

Role-Based Security



General Employee

- Handle Information Responsibly
- Use Good Cyber Behavior
- Report Suspicious Activity/ Mistakes

Managers/ Supervisors

- Initiate Incident Response Plan
- Communicate Appropriately
- Gather Accurate, Pertinent Information
- Review Efforts and Incident

IT Personnel

- Diagnose and Scope the Threat/ Incident
- Engage in Mitigations/ Recovery
- Communicate with Managers/ Supervisors on Timeline
- Guide 3rd Party Assistance
- Document Efforts and Incident

Insider Threat

3.2.3	**SECURITY REQUIREMENT** Provide security awareness training on recognizing and reporting potential indicators of insider threat.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.2.3[a] *potential indicators associated with insider threats are identified.*
	3.2.3[b] *security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Security awareness and training policy; procedures addressing security awareness training implementation; security awareness training curriculum; security awareness training materials; insider threat policy and procedures; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel that participate in security awareness training; personnel with responsibilities for basic security awareness training; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms managing insider threat training].

3.2.3 – Meeting the Controls

SECURITY AWARENESS AND TRAINING	3.2.3[a] potential indicators associated with insider threats are identified.
RESPONSIBILITY MATRIX SECURITY AWARENESS AND TRAINING	3.2.3[b] security awareness training on recognizing and reporting potential indicators of insider threat is provided to managers and employees.

Documentation & Evidence

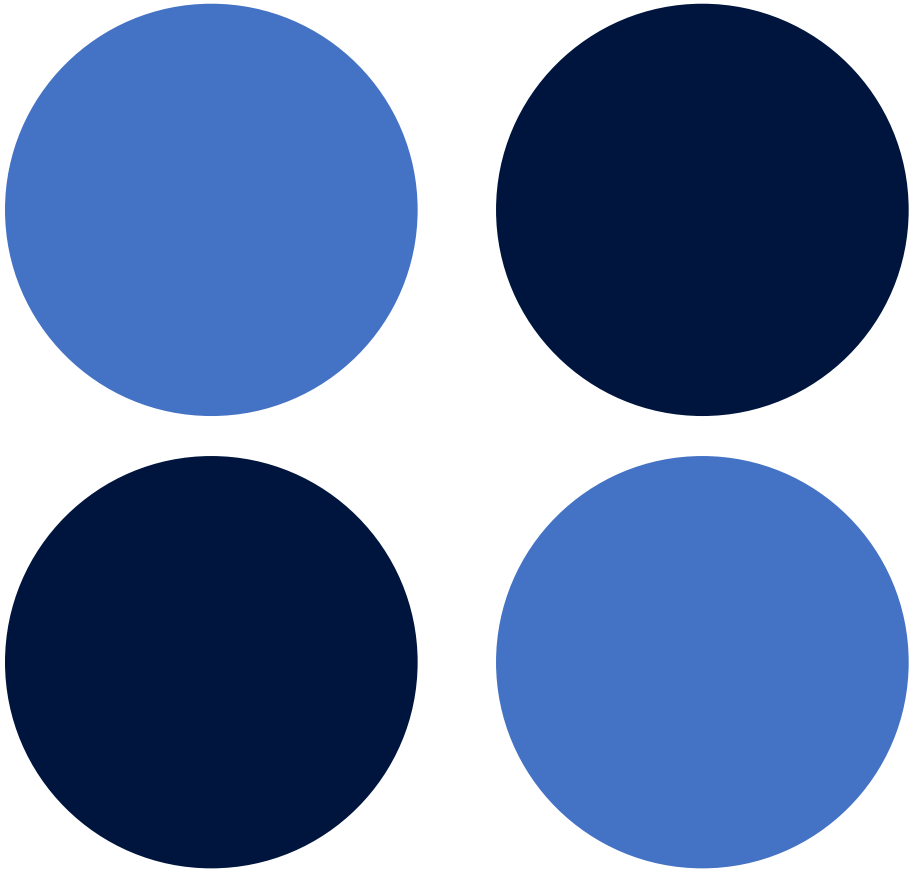
1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

System Security Plan

Control Owners
are clearly defined.



Technical Control Artifacts
are collected, accurate, and available.

Processes
are documented and approved.

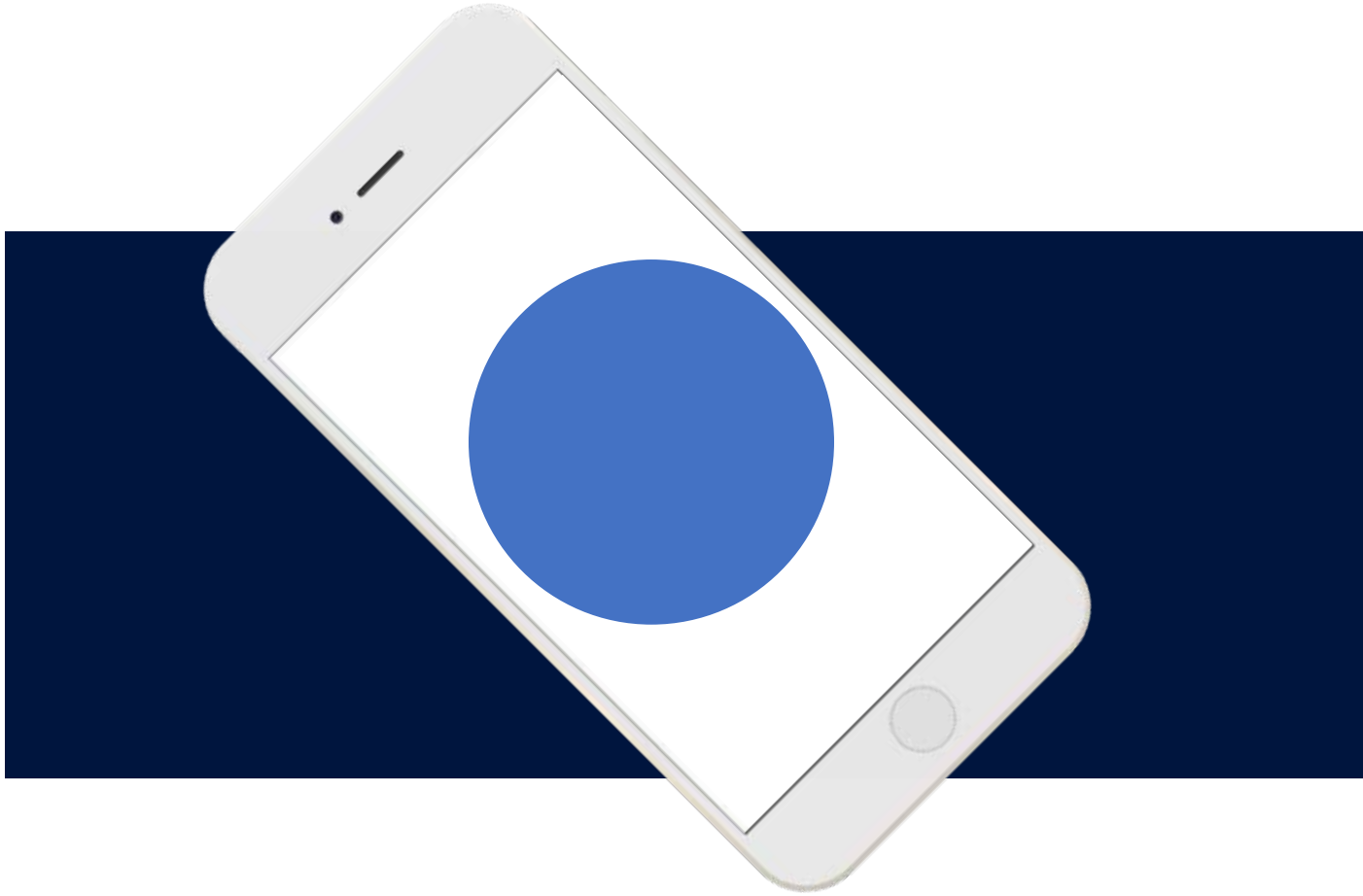
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR

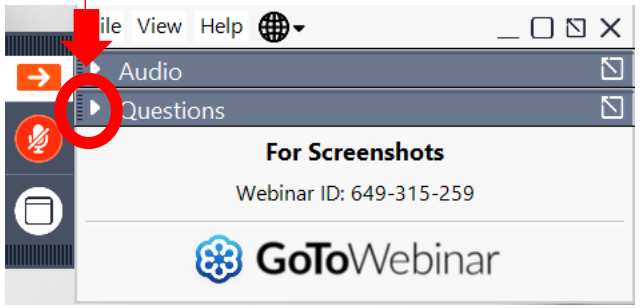


APEX ACCELERATORS

QUESTIONS?

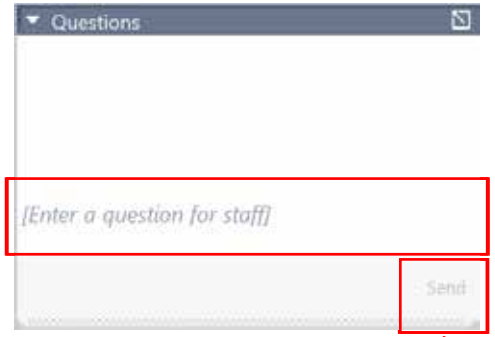
OPENING THE QUESTIONS BOX

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

CYBER FRIDAY LIVE WEBINAR SERIES

- September 15
  NIST SP 800.171 – 3.2 – Awareness & Training and 3.3 Audit & Accountability
- September 22
  NIST SP 800.171 – 3.4 Configuration Management and 3.5 Identification & Authentication
- October 6
  NIST SP 800.171 – 3.6 Incident Response
- October 20
  NIST SP 800.171 – 3.7 Maintenance and 3.8 Media Protection
- October 27
  NIST SP 800.171 – 3.9 Personnel Security and 3.10 Physical Protection

PRESENTED BY

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR
Cyber Friday

TECHNOLOGY INNOVATION CENTER at RESEARCH PARK

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

APEX ACCELERATORS

MENTOR PROTÉGÉ

Coaching Small Business Champions

September 20, 2023

Guest Speaker:

Mark Webster, Mark Webster Communication, Branding: Finding + Telling Your Story

Program also includes:

2025 NFL Draft: Update on Opportunities | Government-Market Opportunities Update | Networking & Buyer Meetings

More info at wispro.org/events

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

September 5, 2023

- Registration Open -

December 5-7, 2023

Register at MarketplaceWisconsin.com

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

September 15, 2023

SURVEY

CONTINUING PROFESSIONAL EDUCATION

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

Jack Laufenberg
jackl@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Matthew Frost
Wisconsin Procurement Institute
mattf@wispro.org | 608.293.0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226