Cyber Friday:

NIST SP 800.171 3.11 Risk Assessment and 3.12 Security Assessment

November 3| 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

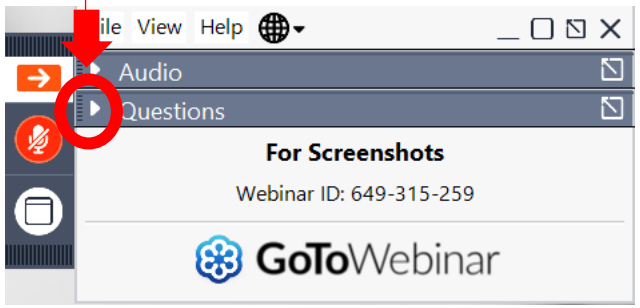
THANK YOU!

Wisconsin Procurement Institute

NCMA WISCONSIN

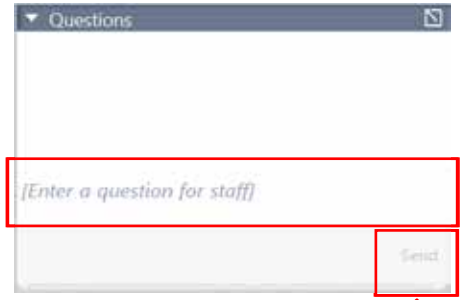
OPENING THE QUESTIONS BOX

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

NCMA WISCONSIN

Wisconsin Procurement Institute

APEX ACCELERATORS

Assisting Wisconsin businesses compete in the government marketplace.

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.

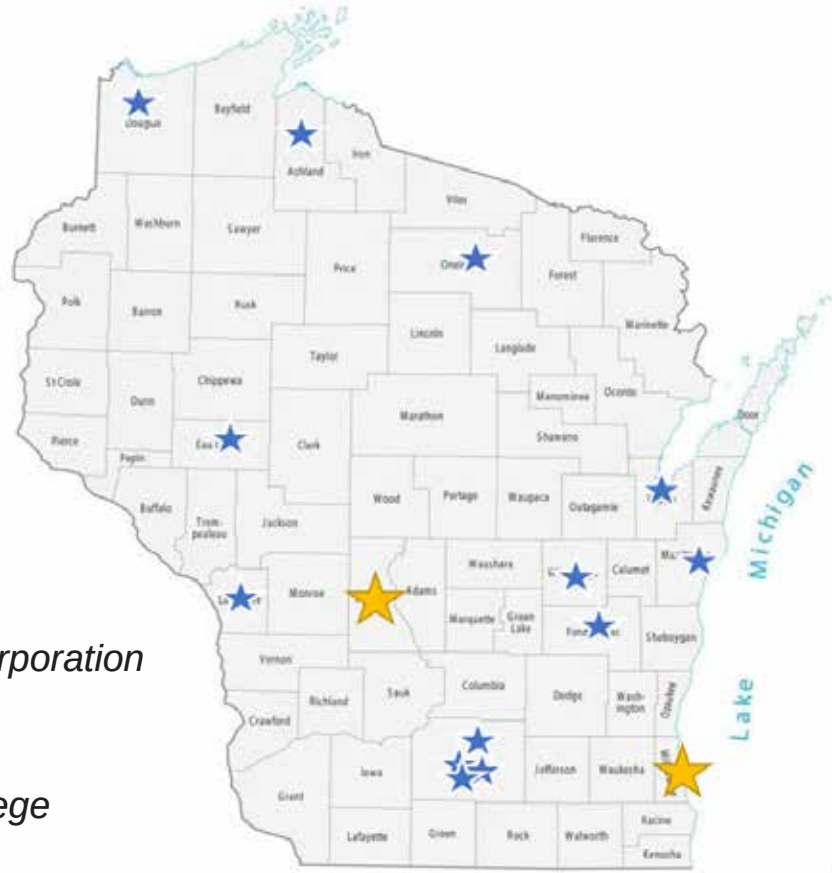
WPI provides services to all of Wisconsin's 72 counties

- 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

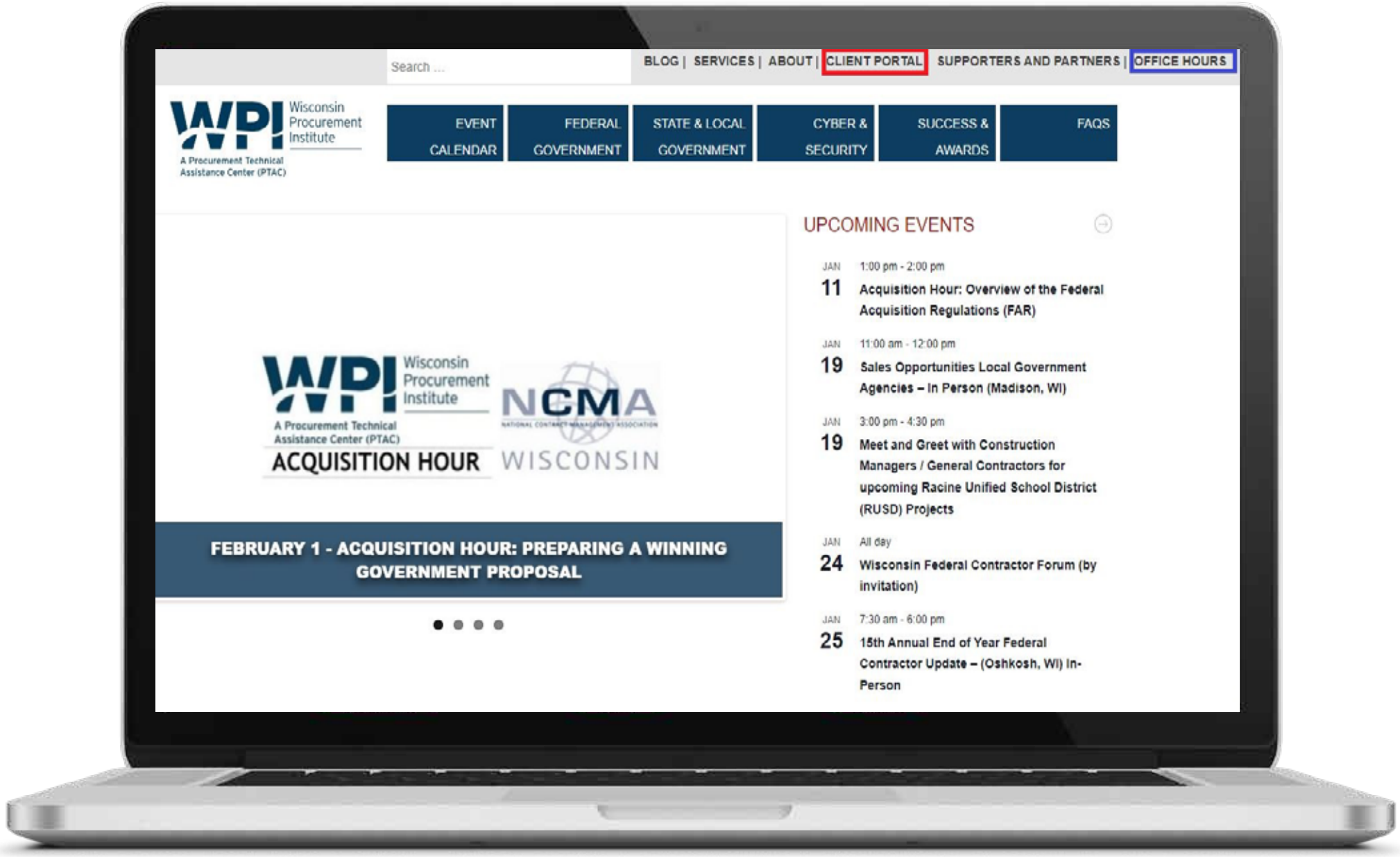
WPI OFFICE LOCATIONS

- **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*



WPI Wisconsin Procurement Institute

NCMA WISCONSIN



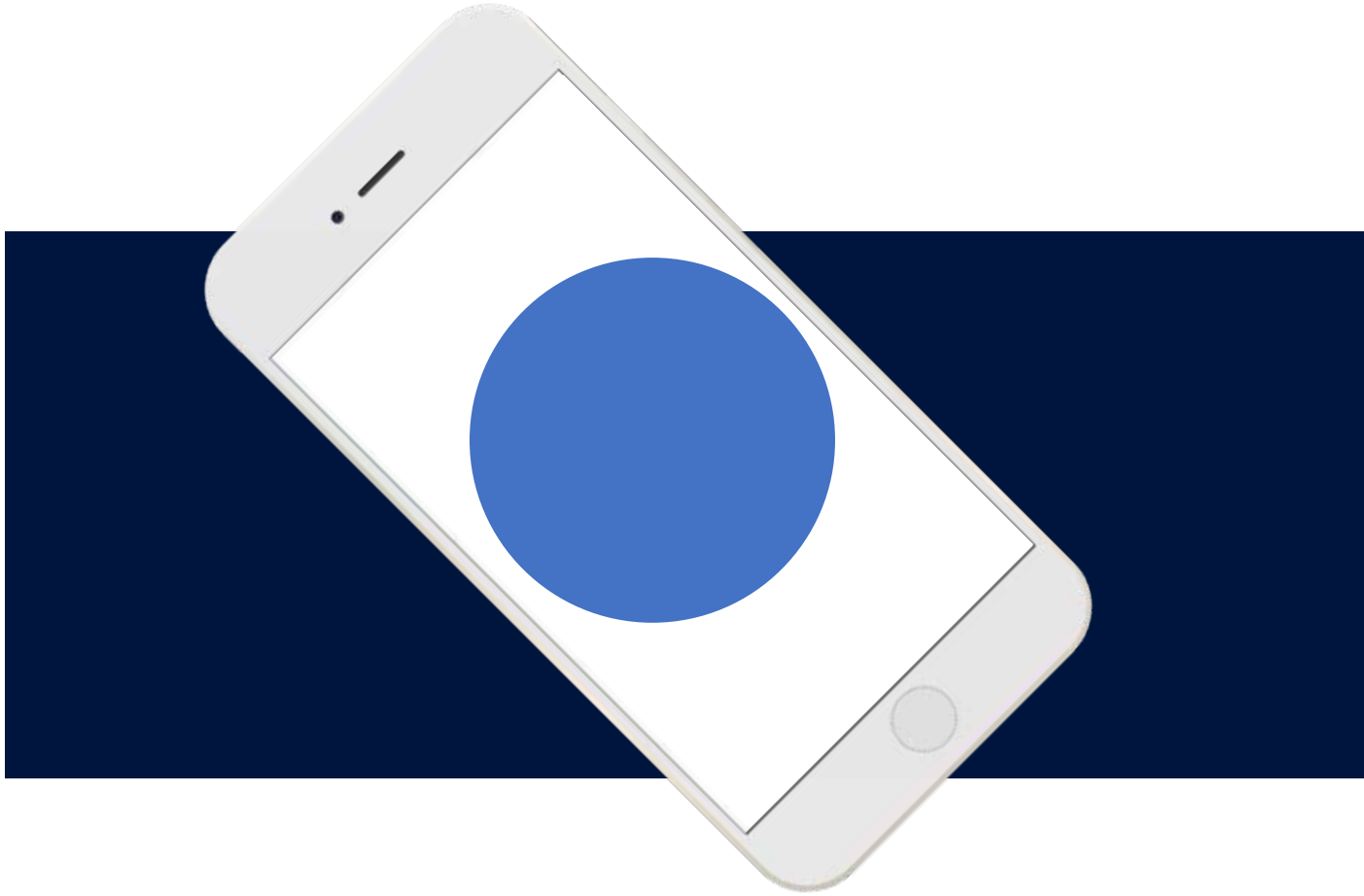
WPI Wisconsin Procurement Institute APEX

NCMA WISCONSIN

Introduction to NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – November 3rd, 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.

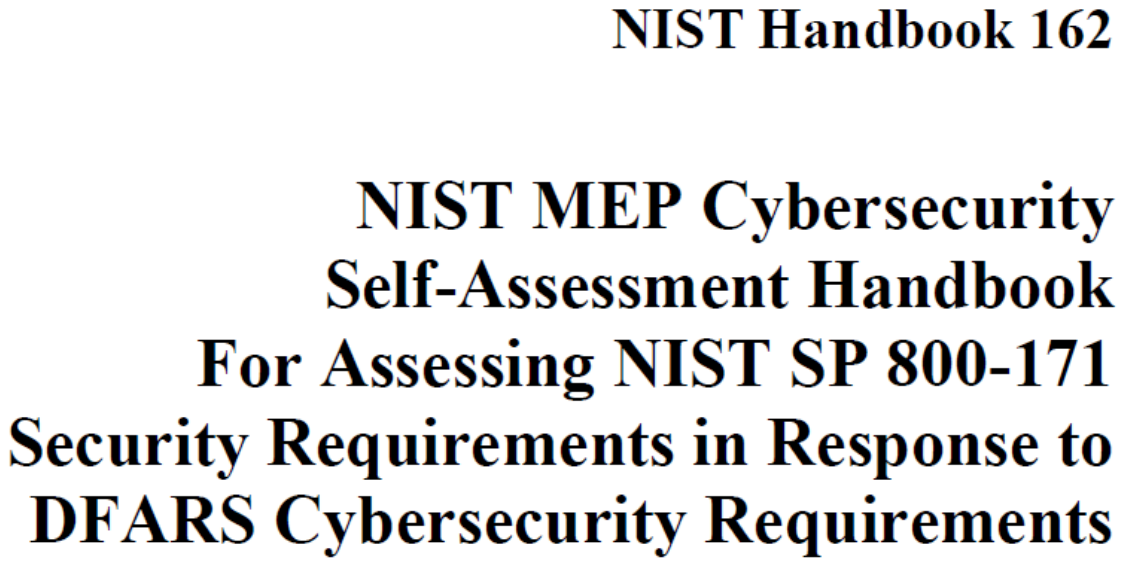
DFARS 252.204-7021

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



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 800-171r2

NIST Special Publication 800-171 Revision 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Reading the Controls

1 — Understanding the Controls

2 — Controls & Objectives

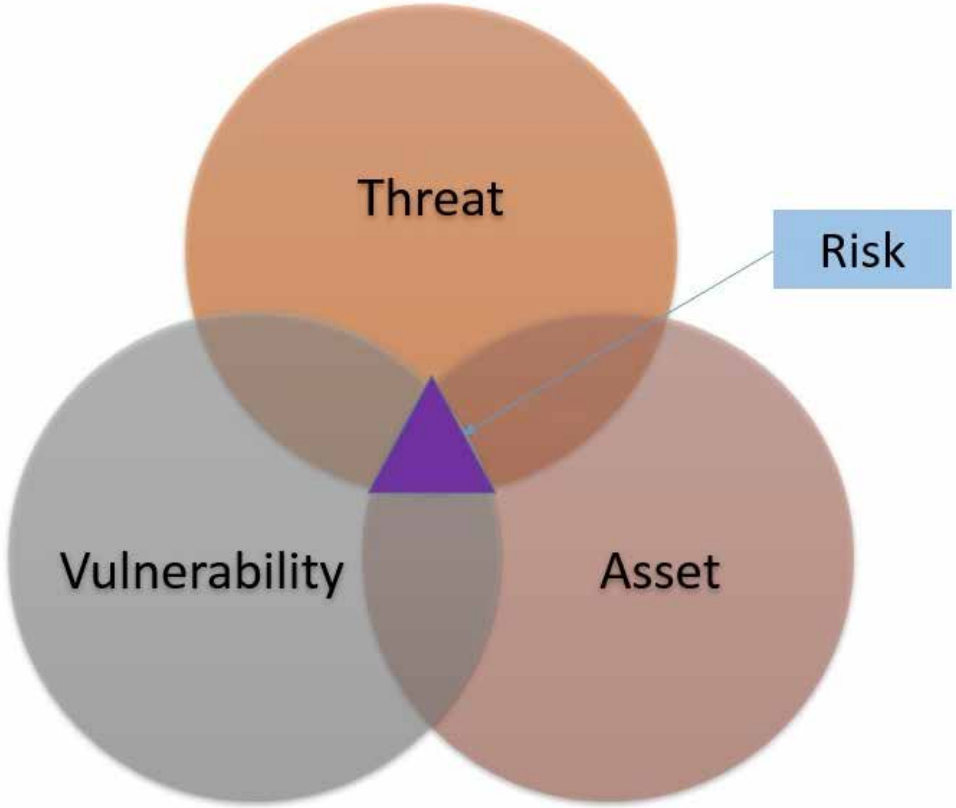
3 — Documentation & Evidence

Risk vs Security

RISK

- Examines Threats
- Examines Vulnerabilities
- Examines Impact

Designed to evaluate what could / should happen.



SECURITY

- Examines Controls
- Examines Behavior
- Examines Implementation

Designed to evaluate what is happening / not happening.

3.11.1 **Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.**

DISCUSSION

Clearly defined system boundaries are a prerequisite for effective risk assessments. Such risk assessments consider threats, vulnerabilities, likelihood, and impact to organizational operations, organizational assets, and individuals based on the operation and use of organizational systems. Risk assessments also consider risk from external parties (e.g., service providers, contractors operating systems on behalf of the organization, individuals accessing organizational systems, outsourcing entities). Risk assessments, either formal or informal, can be conducted at the organization level, the mission or business process level, or the system level, and at any phase in the system development life cycle.

3.10 Risk Assessment

Scope

Policy/Intent

Threats

Mitigation

3.12.1 **Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.**

DISCUSSION

Organizations assess security controls in organizational systems and the environments in which those systems operate as part of the system development life cycle. Security controls are the safeguards or countermeasures organizations implement to satisfy security requirements. By assessing the implemented security controls, organizations determine if the security safeguards or countermeasures are in place and operating as intended. Security control assessments ensure that information security is built into organizational systems; identify weaknesses and deficiencies early in the development process; provide essential information needed to make risk-based decisions; and ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls as documented in system security plans.

Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted.

3.11 Security Assessment

Determine Accuracy

Ensure Process Integrity

Discover Gaps And Divergences

POAM Findings

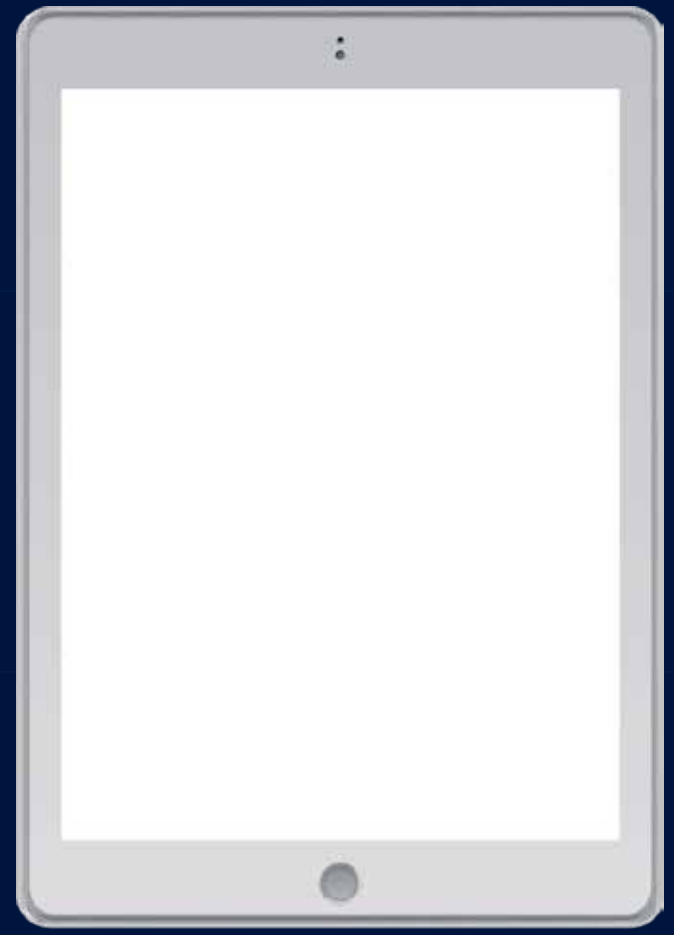
Controls & Objectives

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

Risk Assessment



The Assessment

- Risk Assessment Policy
- Risk and Security Assessment Plan
- Supporting Documentation Review
- Vulnerability Scanning

Assessment Findings

- Vulnerability Mitigation Plan
- Security Review
- Security Team Briefing

Updating Documentation

- SSP Implementation Statement Update
- Vulnerability Resolution
- Updating POAM

3.11.1	**SECURITY REQUIREMENT** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.1[a]	*the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.*
	3.11.1[b]	*risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].	

3.11.1 – Meeting the Controls

RISK ASSESSMENT POLICY

3.11.1[a] the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.

3.11.1[b] risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.

Include forms/documentation in process that speak to risk evaluation.

Include formal intention of assessment schedule.

3.11.2	SECURITY REQUIREMENT Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.11.2[a] *the frequency to scan for vulnerabilities in organizational systems and applications is defined.*
	3.11.2[b] *vulnerability scans are performed on organizational systems with the defined frequency.*
	3.11.2[c] *vulnerability scans are performed on applications with the defined frequency.*
	3.11.2[d] *vulnerability scans are performed on organizational systems when new vulnerabilities are identified.*
	3.11.2[e] *vulnerability scans are performed on applications when new vulnerabilities are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].

3.11.2 – Meeting the Controls

Vulnerability Scanning Process

3.11.2[a] the frequency to scan for vulnerabilities in organizational systems and applications is defined.

3.11.2[b] vulnerability scans are performed on organizational systems with the defined frequency.

3.11.2[c] vulnerability scans are performed on applications with the defined frequency.

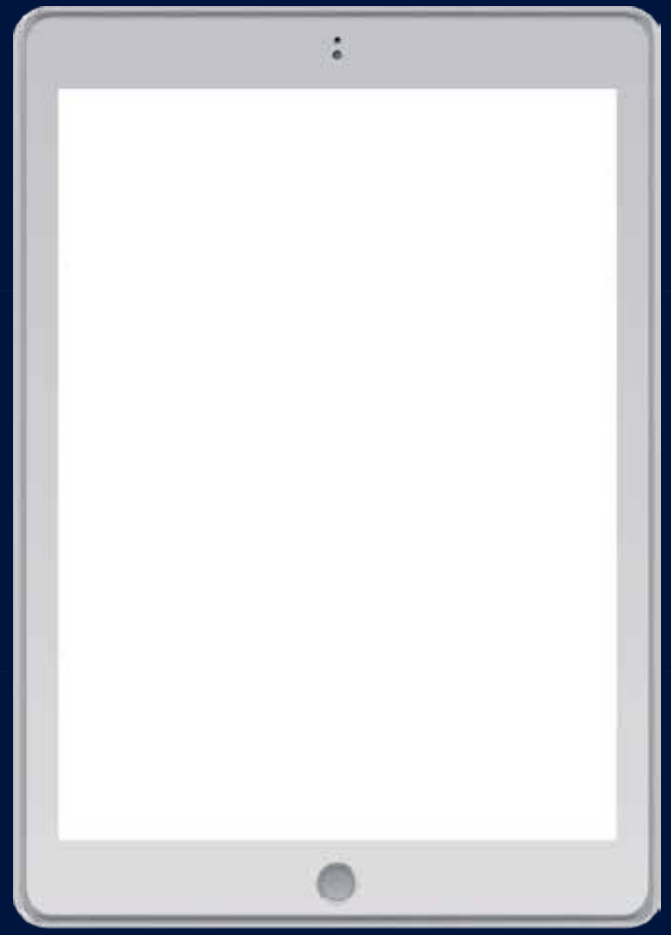
3.11.2[d] vulnerability scans are performed on organizational systems when new vulnerabilities are identified.

3.11.2[e] vulnerability scans are performed on applications when new vulnerabilities are identified.

Include schedule for vulnerability scans using utility.

Include ad-hoc process for when new critical vulnerabilities are announced.

Risk Assessment



The Assessment

- Security Assessment Policy
- Risk and Security Assessment Plan
- Supporting Documentation Review
- Control Process Review

Assessment Findings

- Gap Analysis
- Security Review
- Security Team Briefing

Updating Documentation

- SSP Implementation Statement Update
- Process Changes Documented
- Updating POAM

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.12.1[a] *the frequency of security control assessments is defined.*
	3.12.1[b] *security controls are assessed with the defined frequency to determine if the controls are effective in their application.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with security assessment responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].

3.12.1 – Meeting the Controls

SECURITY ASSESSMENT POLICY

3.12.1[a] the frequency of security control assessments is defined.

3.12.1[b] security controls are assessed with the defined frequency to determine if the controls are effective in their application.

Include forms/documentation in process that and behavior/interview component.

Include formal statement on effectiveness.

3.12 Steps of a Security Assessment

Control Review

Policy & Process Review

Behavioral Interview & Review

Assess & Record

3.12 Steps of a Security Assessment

What should we be doing?

What did we say we would do?

What are we doing?

Are we doing it? Is it effective?

3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.12.2[a]	*deficiencies and vulnerabilities to be addressed by the plan of action are identified.*
	3.12.2[b]	*a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	3.12.2[c]	*the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Mechanisms for developing, implementing, and maintaining plan of action].	

3.12.2 – Meeting the Controls

PLAN OF ACTIONS AND MILESTONES

3.12.2[a] deficiencies and vulnerabilities to be addressed by the plan of action and milestones are identified.

3.12.2[b] a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

3.12.2[c] the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.

Upon discovery of GAP between control intention and implementation/effectiveness.

NIST Control Number	Control	Responsible Office	Scheduled Completion Date	Milestones with Interim Completion Dates	Changes to Milestones	Status
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).					Ongoing

Documentation & Evidence

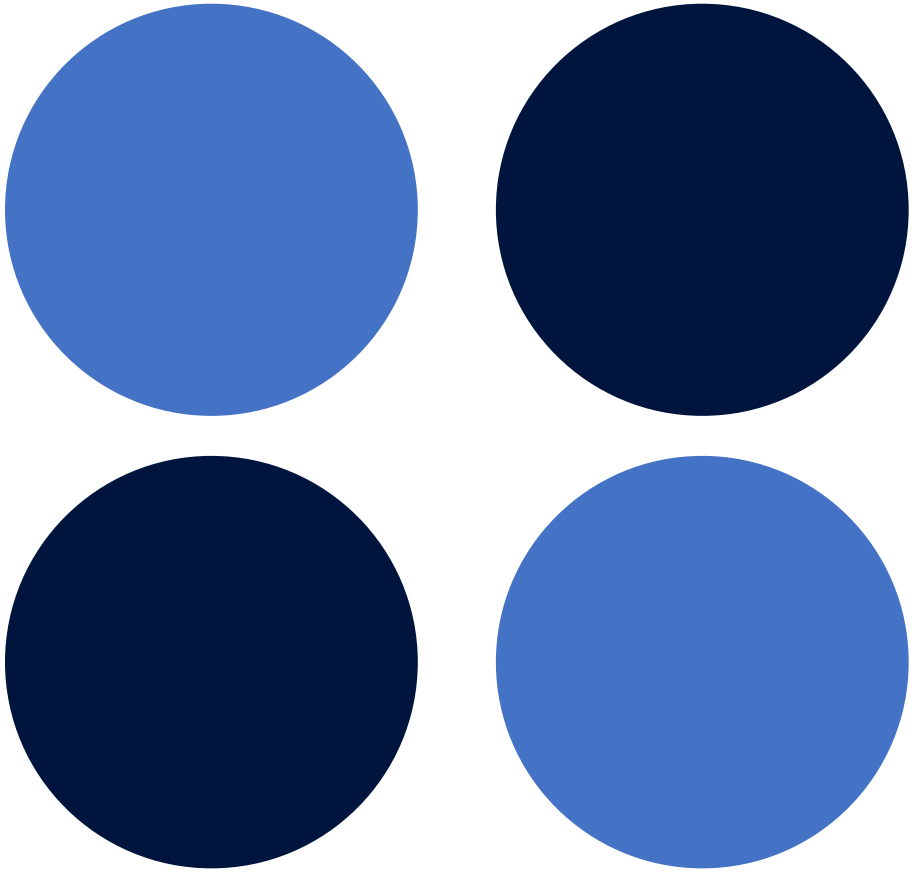
1 Understanding the Controls

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.

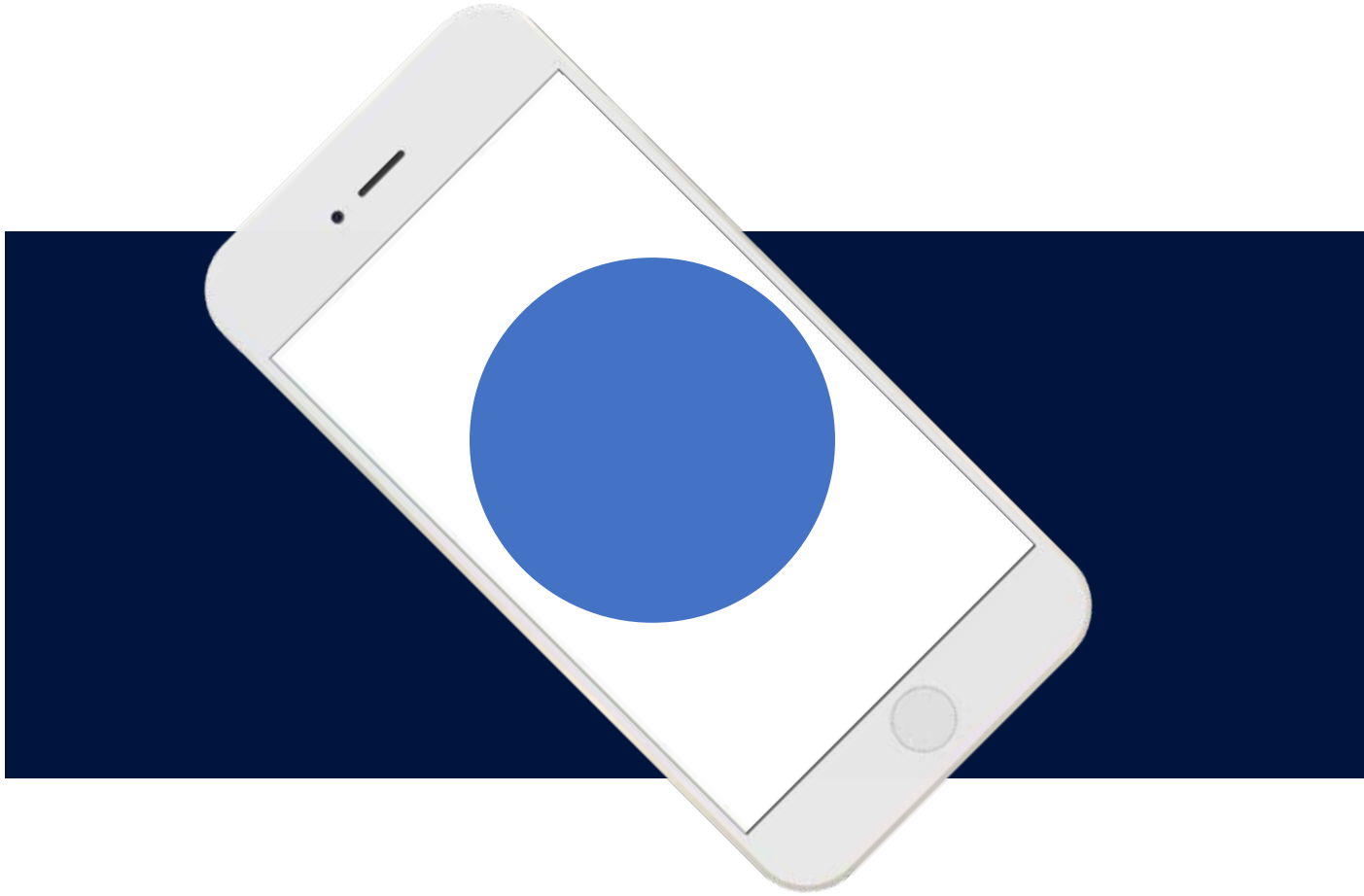
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

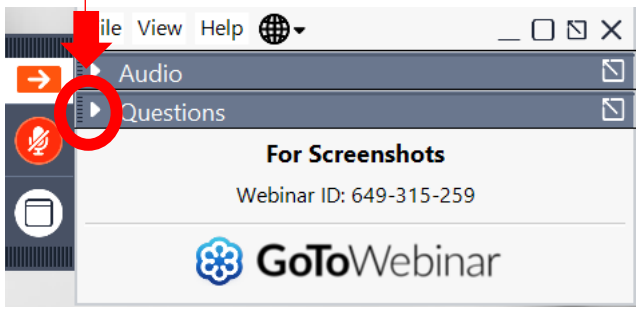
AN APEX ACCELERATOR



QUESTIONS?

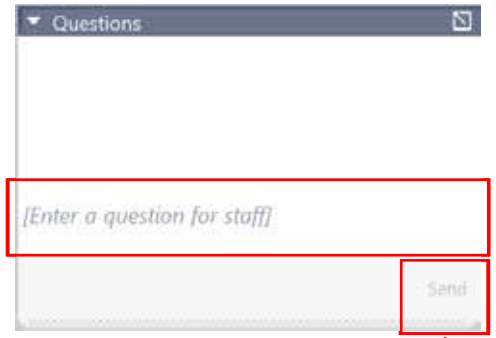
OPENING THE QUESTIONS BOX

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

GOVERNMENT CERTIFICATION WORKSHOPS

- ~~October 12~~
  ~~Federal Certifications~~
- ~~October 26~~
  ~~Local Certifications~~
- November 30
  State Certifications

MADISON AREA TECHNICAL COLLEGE

MATC Goodman-South Campus
2429 Perry Street, Madison, WI 53713

…More information and registrations at wispro.org/events

CYBER FRIDAY LIVE WEBINAR SERIES

- ~~October 27~~
  ~~NIST SP 800.171 – 3.9 Personnel Security and 3.10 Physical Protection~~

- November 3
  NIST SP 800.171 – 3.11 Risk Assessment and 3.12 Security Assessment

- November 9 (Thursday)
  NIST SP 800.171 – 3.13 System and Communications Protection and 3.14 System and Information Integrity

PRESENTED BY

WPI Wisconsin Procurement Institute
APEX Accelerators
Cyber Friday

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

Registration Now Open

The Contracting Academy

Developing and Growing Government Contractors

December 5-7, 2023

MarketplaceWisconsin.com

November 3, 2023

Registration Now Open

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

WPI Wisconsin Procurement Institute APEX ACCELERATORS

Announcing 2024

Evening FAR Sessions

Wispro.org/Events

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

November 3, 2023

SURVEY

Wisconsin Procurement Institute

November 3, 2023

NCMA WISCONSIN

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

Matt Frost

Wisconsin Procurement Institute

mattf@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226