Wisconsin Procurement Institute
AN APEX ACCELERATOR

APEX ACCELERATORS

Cyber Friday:
NIST SP 800.171 – 3.1 – Access Control

September 8 | 11:00 am – Noon
Presented by Matt Frost, WPI

Wisconsin Procurement Institute
Cyber Friday

Webinar Etiquette

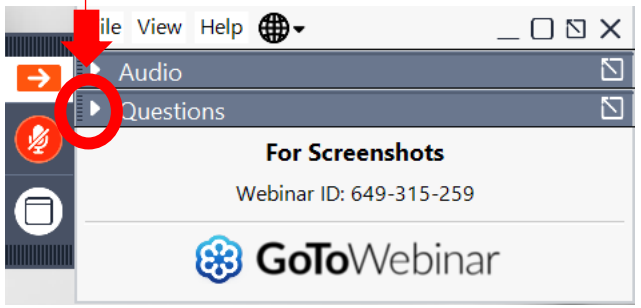
PLEASE

- § 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!

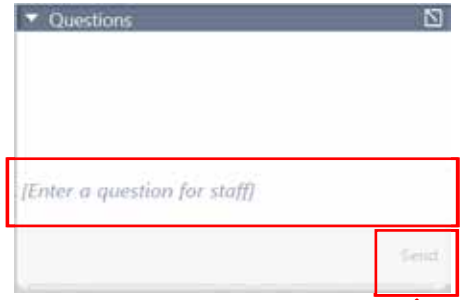
OPENING THE QUESTIONS BOX

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.

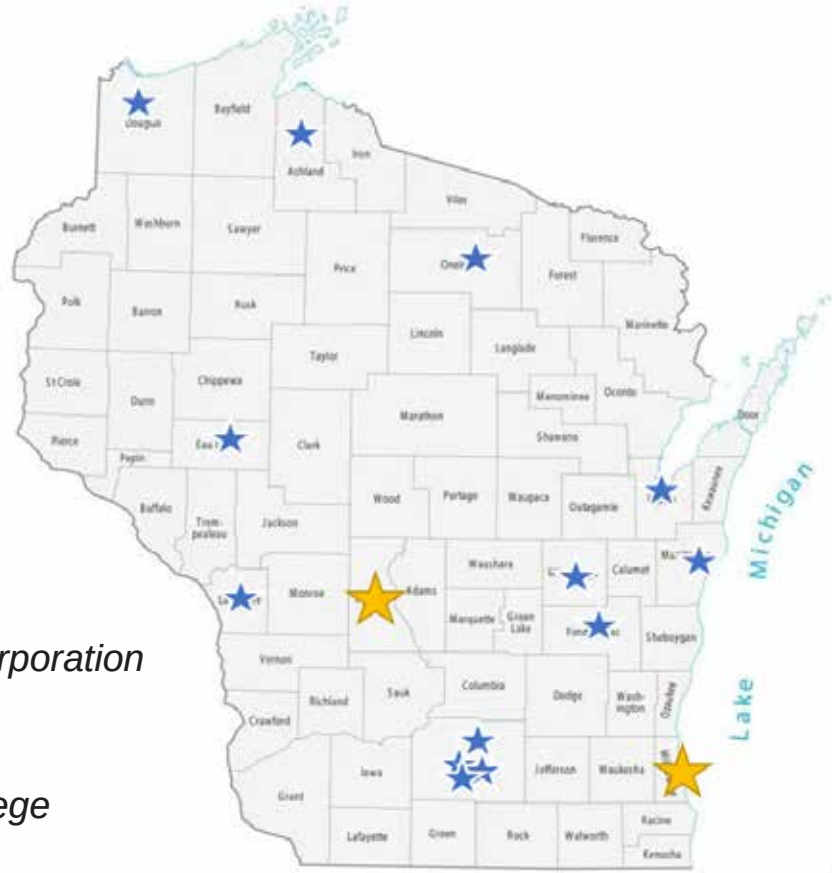
WPI provides services to all of Wisconsin's 72 counties

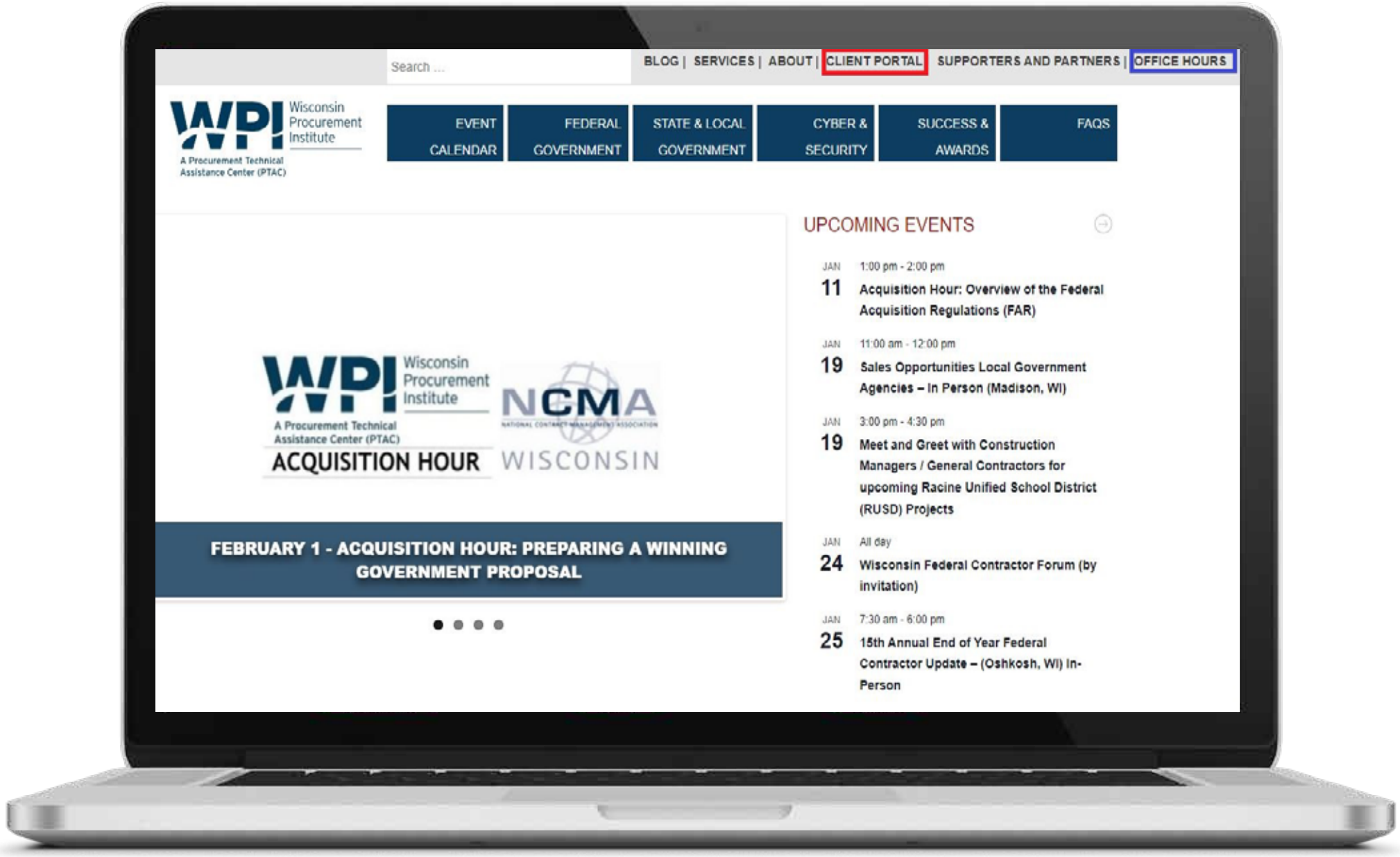
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays,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

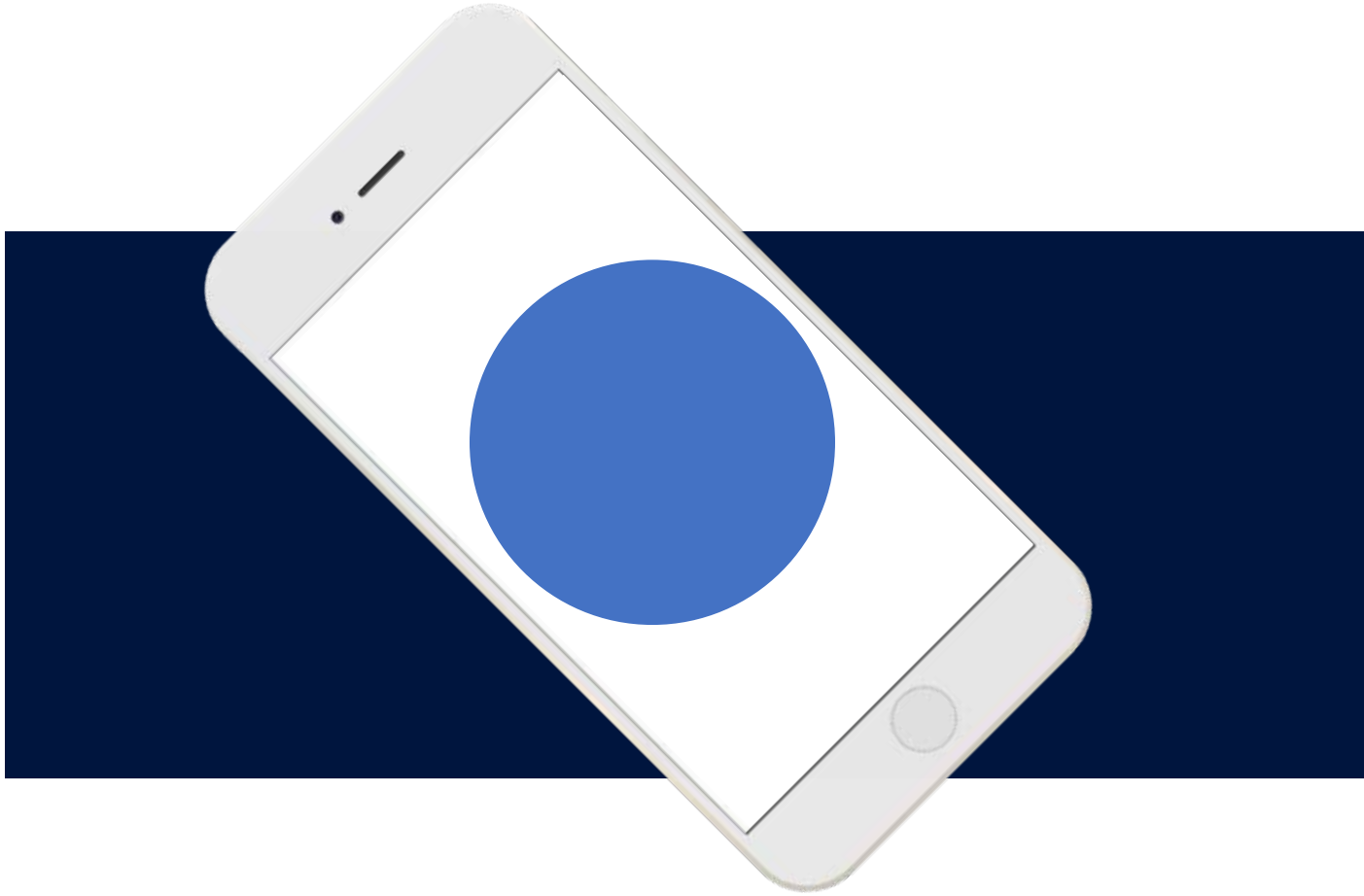



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL | SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
Wisconsin Procurement Institute
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 8th, 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.

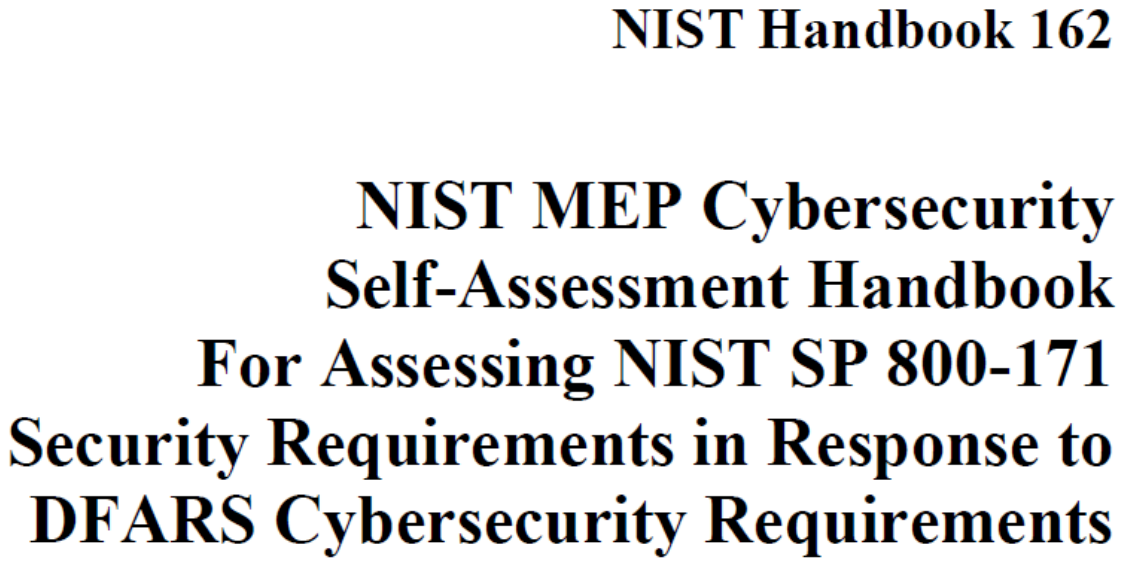
DFARS 252.204-7021

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 800-18r1

NIST Special Publication 800-18
Revision 1
Guide for Developing Security Plans for Federal Information Systems

Reading the Controls

1 — Reading the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

3.1.1 **Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).**

DISCUSSION

Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2.

3.1.1	**SECURITY REQUIREMENT** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.1[a] *authorized users are identified.*
	3.1.1[b] *processes acting on behalf of authorized users are identified.*
	3.1.1[c] *devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d] *system access is limited to authorized users.*
	3.1.1[e] *system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f] *system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

Control Requirements

Access Control Policies

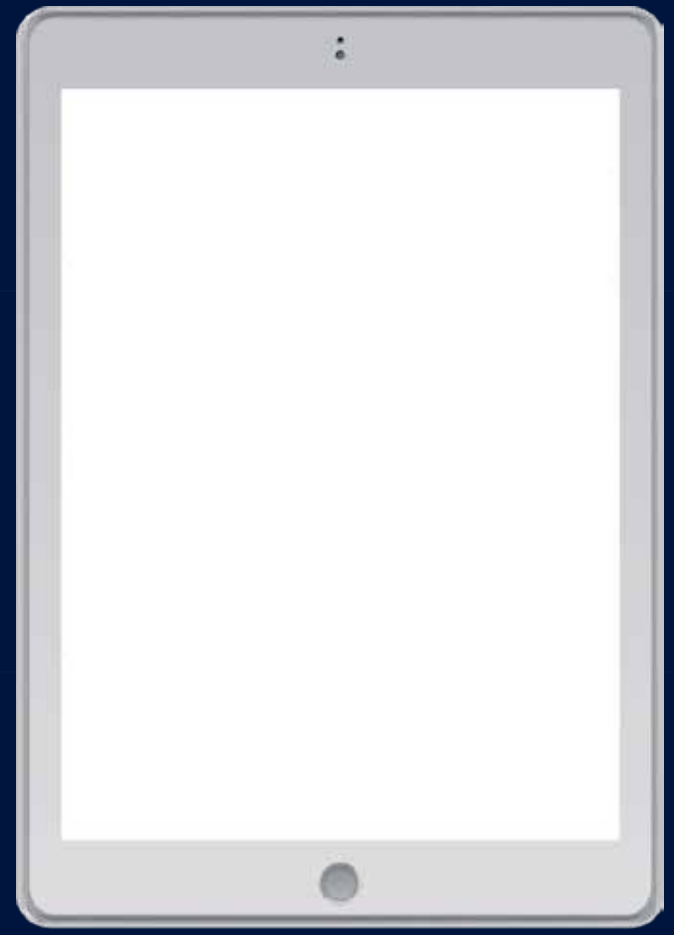
- Acceptable Use Policy
- Account Authorization Form
- System Security Plan
- Onboard / Offboard Procedure

Technical Control / Management

- System Configuration
- Account Records
- Transaction Records

Record Keeping

- Authorization Records
- Account Management Reviews
- System Audit Logs
- Up to Date Account / Host Lists



3.1 Controls

Account Authorization	Permissions	Routing & Session Management	Configuration
3.1.1	3.1.4	3.1.3	3.1.8
3.1.2	3.1.5	3.1.11	3.1.9
3.1.15	3.1.6	3.1.12	3.1.10
3.1.16	3.1.7	3.1.13	3.1.17
3.1.18		3.1.14	3.1.19
3.1.22		3.1.20	3.1.21

Controls & Objectives

1 How To Read a Control

2 Controls & Objectives

3 Documentation & Evidence

Meeting the Controls

Process/Plan

- States Organization Intentions
- Defines Process
- Provides Path to Authorization

Implementation

- Shown through technical or non-technical process
- Can be observed
- Owner of this Control is defined

Enforcement

- Technical Restrictions In Place
- Consequences for Policy Breach Defined

Review

- Periodically Reviewed
- Review is Recorded
- This Review process is demonstrable
- Changes to process/control are subject to scrutiny

Account Authorization

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.1[a] *authorized users are identified.*
	3.1.1[b] *processes acting on behalf of authorized users are identified.*
	3.1.1[c] *devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d] *system access is limited to authorized users.*
	3.1.1[e] *system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f] *system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

3.1.1 – Meeting the Controls

USER ACCOUNT AUTHORIZATION POLICY	**3.1.1[a] Authorized Users are Identified** **3.1.1[d] System is limited to authorized users.**
ACTIVE DIRECTORY	**3.1.1[a] Authorized Users are Identified** **3.1.1[b] Processes acting on behalf of authorized Users are identified** **3.1.1[c] Devices [and other systems] authorized to connect to the system are identified** **3.1.1[d] System access is limited to processes acting on behalf of authorized users.** **3.1.1[e] System access is limited to processes acting on behalf of authorized users.** **3.1.1[f] System access is limited to authorized devices (including other systems).**
HARDWARE/SOFTWARE INVENTORY NETWORK DIAGRAM	**3.1.1[c] Devices (and other systems) authorized to connect to system are identified.**

Permissions

3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.4[a]	*the duties of individuals requiring separation are defined.*
	3.1.4[b]	*responsibilities for duties that require separation are assigned to separate individuals.*
	3.1.4[c]	*access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing separation of duties policy].	

3.1.4 – Meeting the Controls

ACCESS CONTROL POLICY

3.1.4[a] the duties of individuals requiring separation are defined.

3.1.4[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

ACTIVE DIRECTORY

3.1.4[b] responsibilities for duties that require separation are assigned to separate individuals.

3.1.4[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

Routing & Session Management

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.3[a] *information flow control policies are defined.*
	3.1.3[b] *methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c] *designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d] *authorizations for controlling the flow of CUI are defined.*
	3.1.3[e] *approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].

3.1.3 – Meeting the Controls

ACCESS CONTROL POLICY

3.1.3[a] information flow control policies are defined.

3.1.3[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.

3.1.3[c] designated sources and destinations for CUI within the system and between interconnected systems are identified.

3.1.3[d] authorizations for controlling the flow of CUI are defined.

3.1.3[e] approved authorizations for controlling the flow of CUI are enforced.

NETWORK DIAGRAM / BUSINESS PROCESS FLOW

3.1.3[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.

3.1.3[c] designated sources and destinations for CUI within the system and between interconnected systems are identified.

Configuration

3.1.8	**SECURITY REQUIREMENT** Limit unsuccessful logon attempts.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.8[a]	*the means of limiting unsuccessful logon attempts is defined.*
	3.1.8[b]	*the defined means of limiting unsuccessful logon attempts is implemented.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing unsuccessful logon attempts; system security plan; system design documentation; system configuration settings and associated documentation; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with information security responsibilities; system developers; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing access control policy for unsuccessful logon attempts].	

3.1.8 – Meeting the Controls

ACCESS CONTROL POLICY

3.1.8[a] the means of limiting unsuccessful logon attempts is defined.

ACTIVE DIRECTORY

3.1.8[b] the defined means of limiting unsuccessful logon attempts is implemented.

Documentation & Evidence

NIST SP 800-171

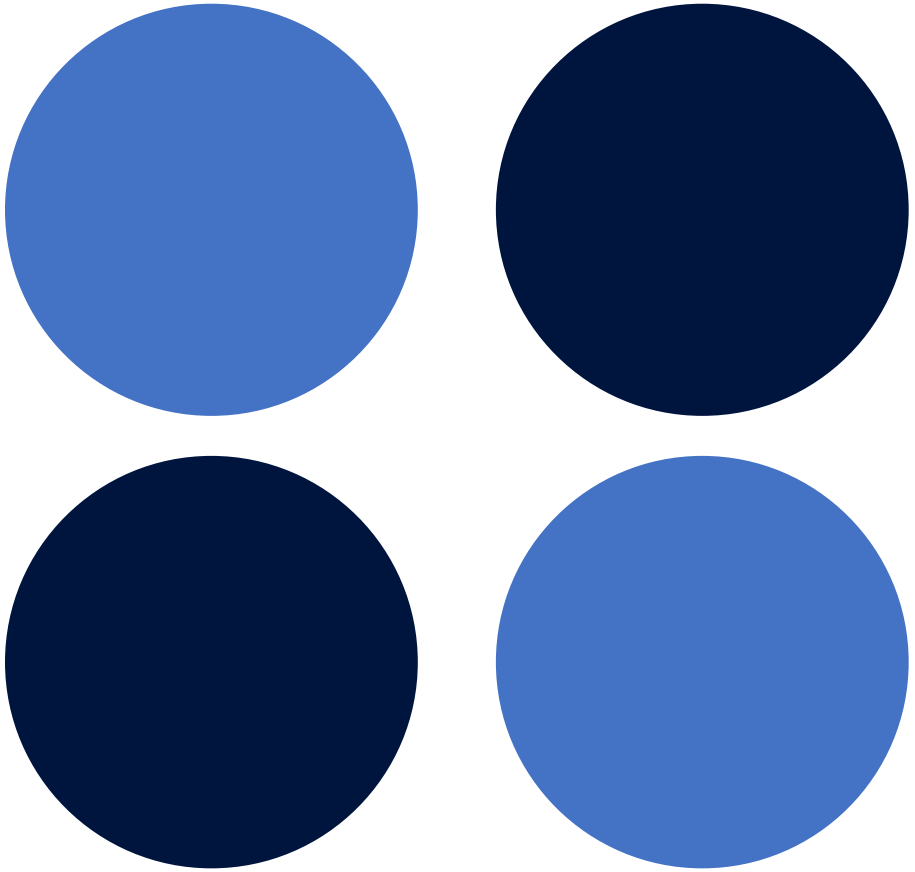
1 How To Read a Control

2 Controls & Objectives

3 Documentation & Evidence

Plan of Action and Milestones

Control Owners
are clearly defined.



Technical Control Artifacts
are collected, accurate, and available.

Processes
are documented and approved.

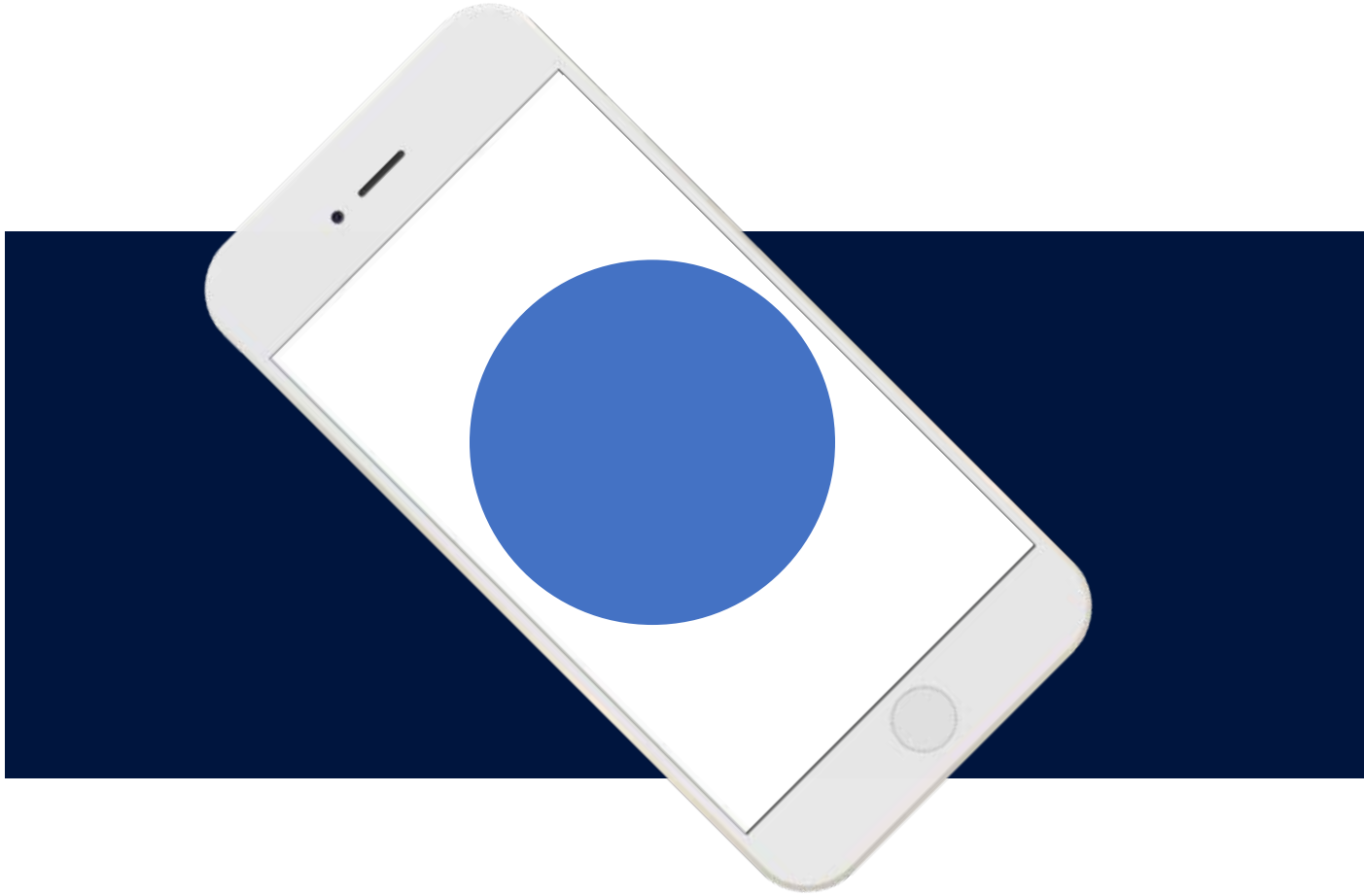
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

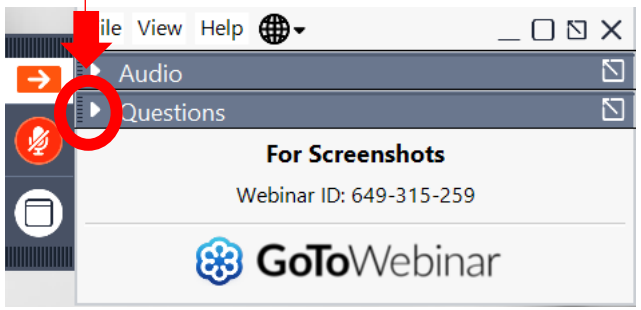
AN APEX ACCELERATOR



QUESTIONS?

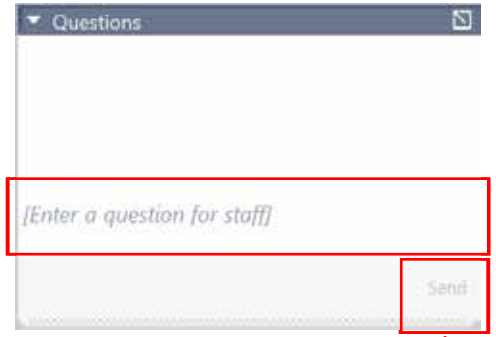
OPENING THE QUESTIONS BOX

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

CYBER FRIDAY LIVE WEBINAR SERIES

- September 8
  NIST SP 800.171 – 3.1 – Access Control
- 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

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

- Save the Date -

December 5-7, 2023

More info coming soon to wispro.org/events

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

SURVEY

Wisconsin Procurement Institute
AN APEX ACCELERATOR

September 8, 2023

APEX ACCELERATORS

CONTINUING PROFESSIONAL EDUCATION

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION®

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