Wisconsin Procurement Institute
AN APEX ACCELERATOR

APEX ACCELERATORS

Cyber Friday:
NIST SP 800.171 – 3.4 Configuration Management and 3.5 Identification & Authentication

September 22 | 11:00 am – Noon
Presented by Matt Frost, WPI

Wisconsin Procurement Institute
Cyber Friday

Webinar Etiquette

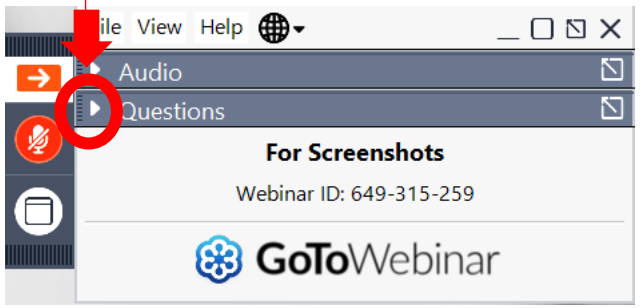
PLEASE

- § 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!

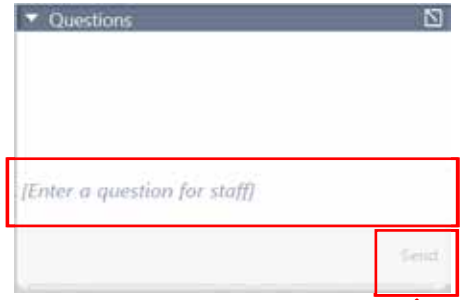
OPENING THE QUESTIONS BOX

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.

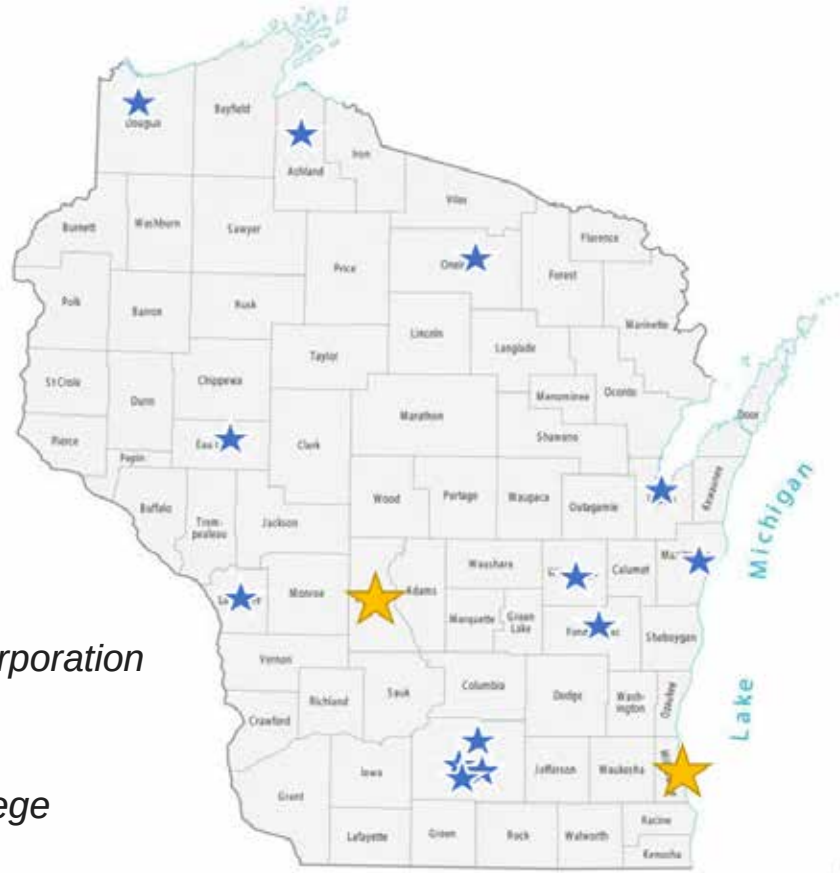
WPI provides services to all of Wisconsin's 72 counties

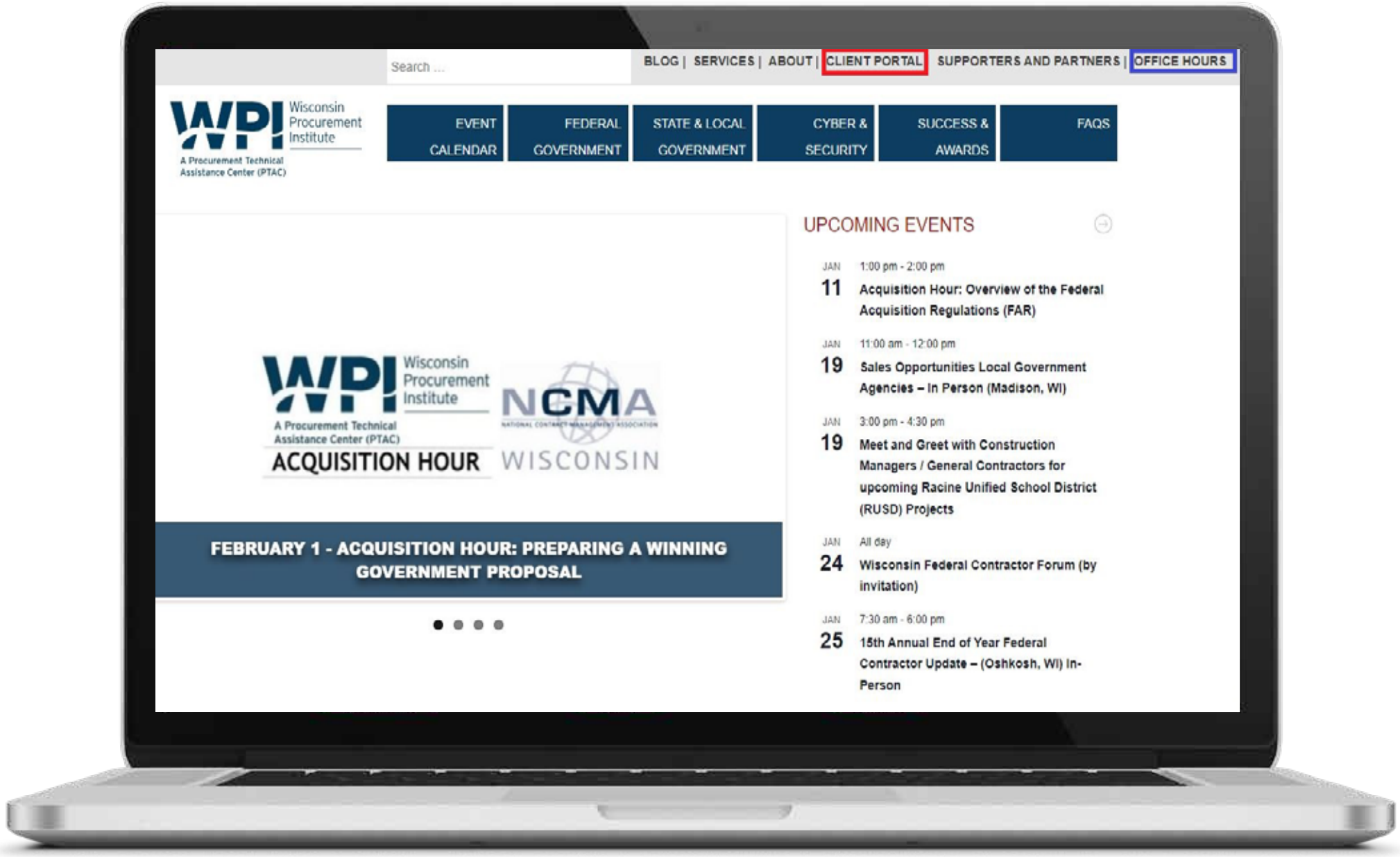
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays,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

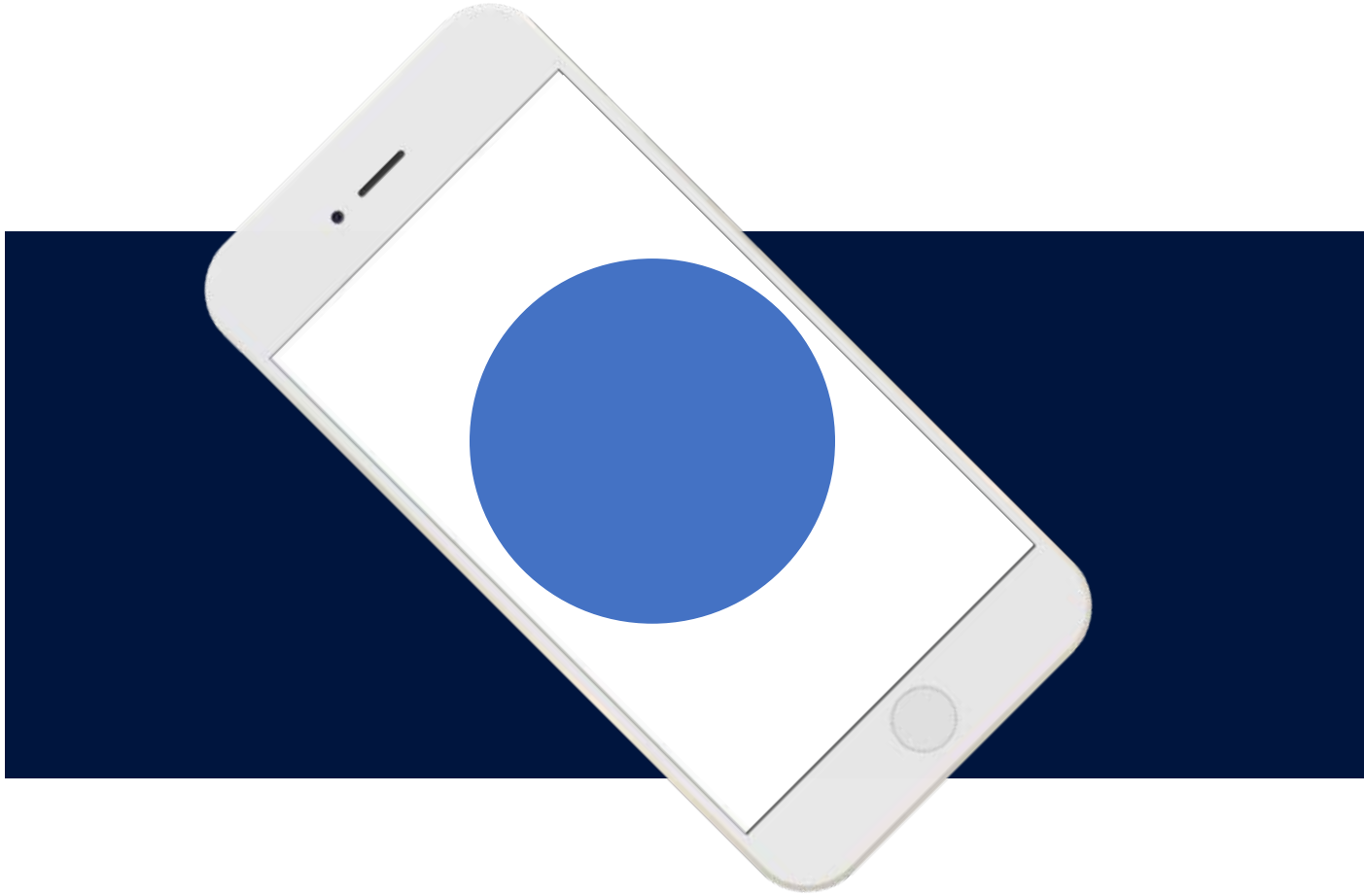



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL | SUPPORTERS AND PARTNERS | OFFICE HOURS
WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
WPI Wisconsin Procurement 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 22nd, 2023

DFARS 252.204-702

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.

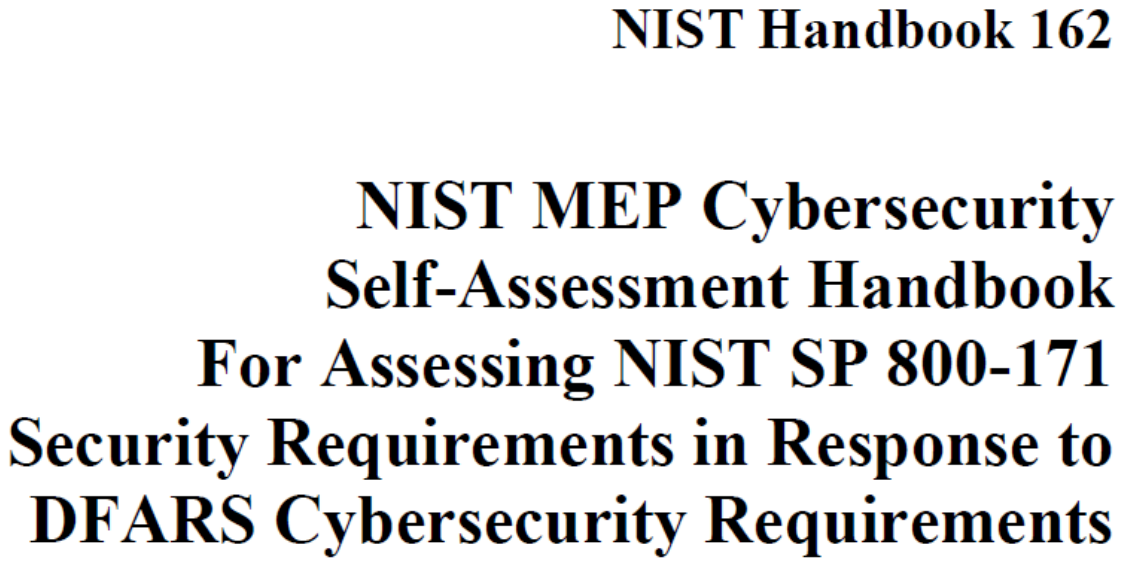
DFARS 252.204-7021

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 800-181r2

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

3.4.1 **Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.**

DISCUSSION

Baseline configurations are documented, formally reviewed, and agreed-upon specifications for systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and changes to systems. Baseline configurations include information about system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and update and patch information on operating systems and applications; and configuration settings and parameters), network topology, and the logical placement of those components within the system architecture. Baseline configurations of systems also reflect the current enterprise architecture. Maintaining effective baseline configurations requires creating new baselines as organizational systems change over time. Baseline configuration maintenance includes reviewing and updating the baseline configuration when changes are made based on security risks and deviations from the established baseline configuration

3.4.1	**SECURITY REQUIREMENT** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

ASSESSMENT OBJECTIVE

Determine if:

3.4.1[a]	*a baseline configuration is established.*
3.4.1[b]	*the baseline configuration includes hardware, software, firmware, and documentation.*
3.4.1[c]	*the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.*
3.4.1[d]	*a system inventory is established.*
3.4.1[e]	*the system inventory includes hardware, software, firmware, and documentation.*
3.4.1[f]	*the inventory is maintained (reviewed and updated) throughout the system development life cycle.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the system; procedures addressing system inventory; system security plan; configuration management plan; system inventory records; inventory review and update records; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system component installation records; system component removal records; other relevant documents or records].

Interview: [*SELECT FROM:* Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsibilities; system or network administrators].

Test: [*SELECT FROM:* Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organizational processes for updating inventory of system components; mechanisms supporting or implementing the system inventory; mechanisms implementing updating of the system inventory].

3.4 Configuration Management

Baseline

Control

Approve

Validate

3.5.1 **Identify system users, processes acting on behalf of users, and devices.**

DISCUSSION

Common device identifiers include Media Access Control (MAC), Internet Protocol (IP) addresses, or device-unique token identifiers. Management of individual identifiers is not applicable to shared system accounts. Typically, individual identifiers are the user names associated with the system accounts assigned to those individuals. Organizations may require unique identification of individuals in group accounts or for detailed accountability of individual activity. In addition, this requirement addresses individual identifiers that are not necessarily associated with system accounts. Organizational devices requiring identification may be defined by type, by device, or by a combination of type/device.

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.5.1[a] *system users are identified.*
	3.5.1[b] *processes acting on behalf of users are identified.*
	3.5.1[c] *devices accessing the system are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers]. **Test**: [*SELECT FROM:* Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability].

3.5 Identification and Authentication

Identify

Restrict

Authorize

Record

Controls & Objectives

NIST SP 800-171

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

Configuration Management

Identify and Strategize

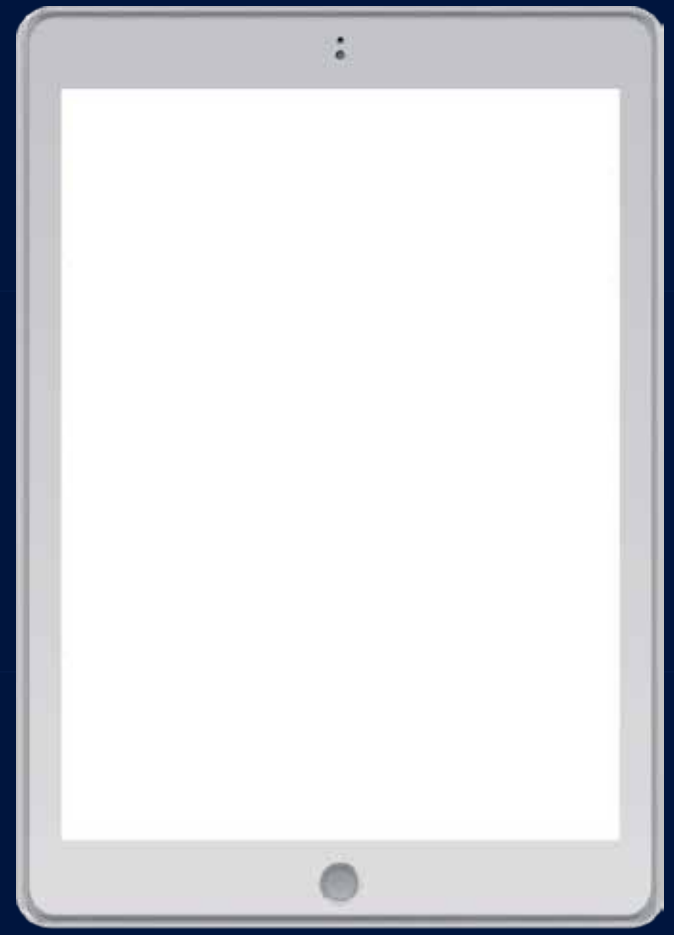
- Role-Based Permissions
- Configure Security Groups / Policy
- Audit Software / Services Against ACL
- Draft Formal Policy

Configure Baseline

- Document Software / Hardware Baselines and Inventory
- Diagram Network Architecture and Business Process
- Expand and Formalize Policy

Lock Down Deployed Solutions

- Deploy Security Groups
- Principle of Least Privilege
- Lock Down Services / Permissions / Rights



Configuration Management

3.4.1	**SECURITY REQUIREMENT** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.1[a]	*a baseline configuration is established.*
	3.4.1[b]	*the baseline configuration includes hardware, software, firmware, and documentation.*
	3.4.1[c]	*the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.*
	3.4.1[d]	*a system inventory is established.*
	3.4.1[e]	*the system inventory includes hardware, software, firmware, and documentation.*
	3.4.1[f]	*the inventory is maintained (reviewed and updated) throughout the system development life cycle.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the system; procedures addressing system inventory; system security plan; configuration management plan; system inventory records; inventory review and update records; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system component installation records; system component removal records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organizational processes for updating inventory of system components; mechanisms supporting or implementing the system inventory; mechanisms implementing updating of the system inventory].	

3.4.1 – Meeting the Controls

HOST BASELINE

INVENTORY

3.4.1[a] a baseline configuration is established

3.4.1[b] the baseline configuration includes hardware, software, firmware, and documentation.

3.4.1[d] a system inventory is established.

3.4.1.[e] the system inventory includes hardware, software, firmware, and documentation.

CONFIGURATION MANAGEMENT POLICY

CHANGE REQUEST PROCESS

3.4.1[c] the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.

3.4.1 [f] the inventory is maintained (reviewed and updated) throughout the system development life cycle.

Configuration Management

3.4.3	**SECURITY REQUIREMENT** Track, review, approve or disapprove, and log changes to organizational systems.

ASSESSMENT OBJECTIVE

Determine if:

3.4.3[a]	*changes to the system are tracked.*
3.4.3[b]	*changes to the system are reviewed.*
3.4.3[c]	*changes to the system are approved or disapproved.*
3.4.3[d]	*changes to the system are logged.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; system security plan; change control records; system audit logs and records; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; other relevant documents or records].

Interview: [*SELECT FROM:* Personnel with configuration change control responsibilities; personnel with information security responsibilities; system or network administrators; members of change control board or similar].

Test: [*SELECT FROM:* Organizational processes for configuration change control; mechanisms that implement configuration change control].

3.24.2 – Meeting the Controls

CONFIGURATION MANAGEMENT POLICY

CHANGE REQUEST PROCESS

TICKETING SYSTEM

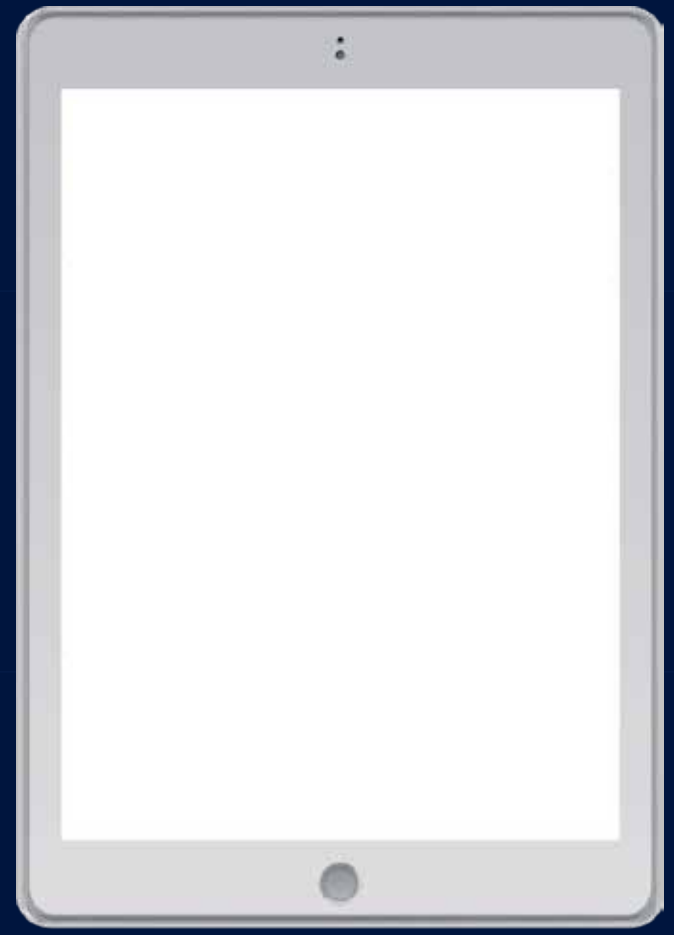
3.4.2[a] changes to the system are tracked.

3.4.2[b] changes to the system are reviewed.

3.4.2[c] changes to the system are approved or disapproved.

3.4.2[d] changes to the system are logged.

Identification & Authentication



Accounts and Services

- Clearly Identified
- Mapped to Individual User / Service / Process
- Logged and Managed

Lock Down Access Controls

- Password Complexity
- MFA
- Additional Security Controls

Document and Review

- Access Control Policy, Acceptable Use Policy, Account Creation Procedures
- Periodically review / audit ACLs and Active Directory
- Validate security is in place and operating as intended

Identification and Authentication

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.5.1[a]	*system users are identified.*
	3.5.1[b]	*processes acting on behalf of users are identified.*
	3.5.1[c]	*devices accessing the system are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers]. **Test**: [*SELECT FROM:* Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability].	

3.5.1 – Meeting the Controls

ACCESS CONTROL POLICY

CONFIGURATION MANAGEMENT POLICY

ACCOUNT REQUEST POLICY

3.5.1[a] system users are identified.

3.5.1[b] processes acting on behalf of users are identified.

HARDWARE INVENTORY

NETWORK DIAGRAM

3.5.1[c] devices accessing the system are identified.

Documentation & Evidence

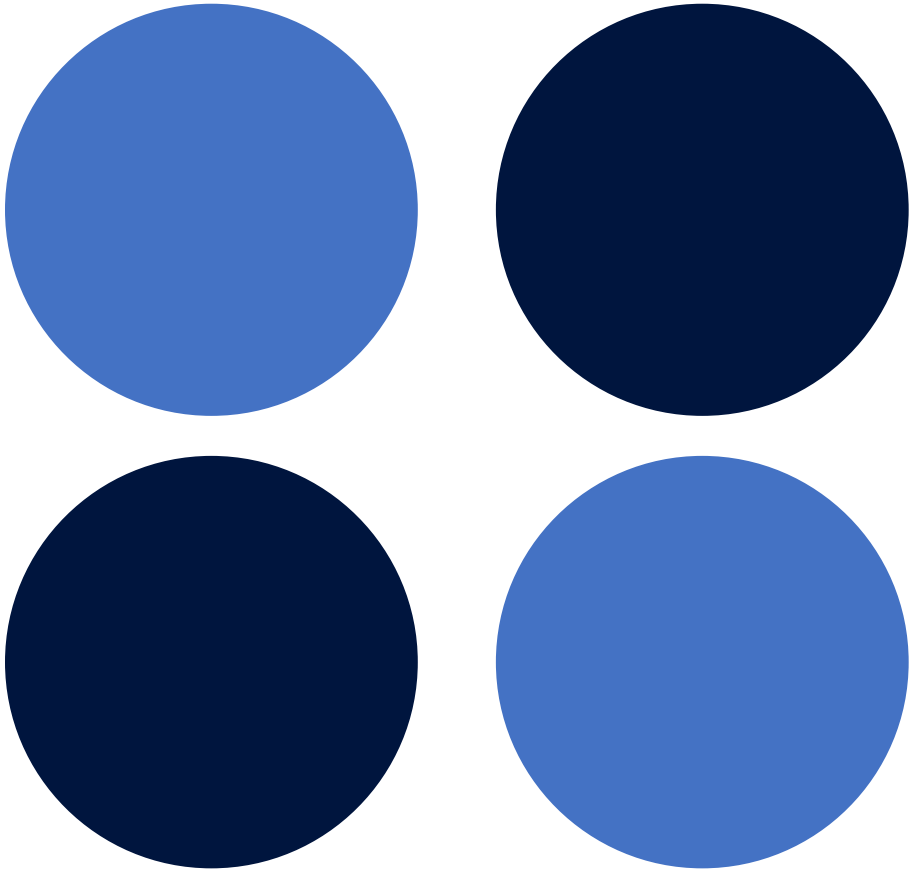
1 — Understanding the Controls

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.

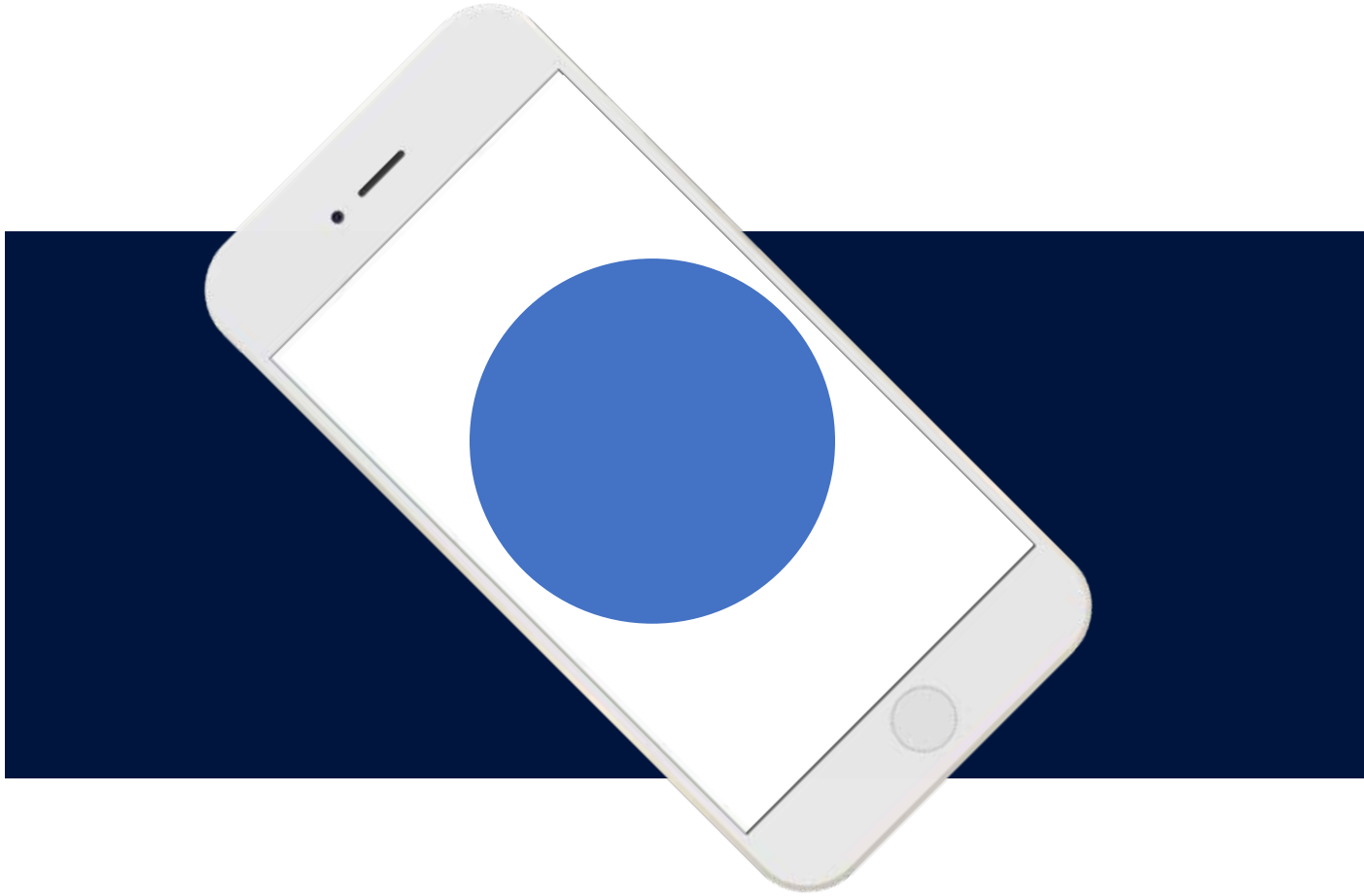
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

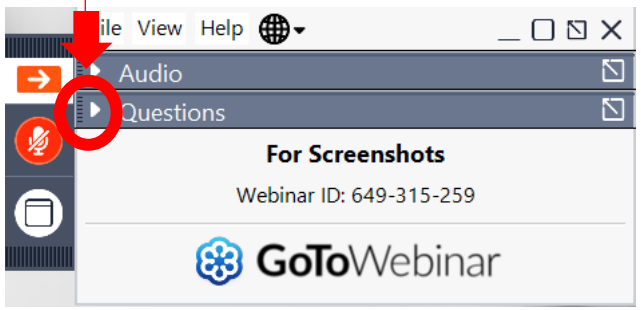
AN APEX ACCELERATOR



QUESTIONS?

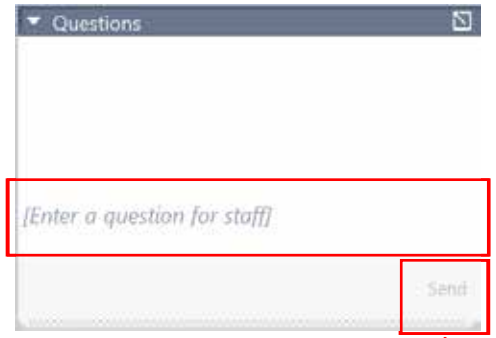
OPENING THE QUESTIONS BOX

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

CYBER FRIDAY LIVE WEBINAR SERIES

- 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
- 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
AN APEX ACCELERATOR
Cyber Friday

TECHNOLOGY INNOVATION CENTER at RESEARCH PARK

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

APEX ACCELERATORS

Registration Now Open

The Contracting Academy

Developing and Growing Government Contractors

December 5-7, 2023

MarketplaceWisconsin.com

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

September 22, 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