Cyber Friday:
NIST SP 800.171 – 3.7 Maintenance and 3.8 Media Protection

October 20| 11:00 am - Noon

Presented by:

Matt Frost, WPI

Webinar Etiquette

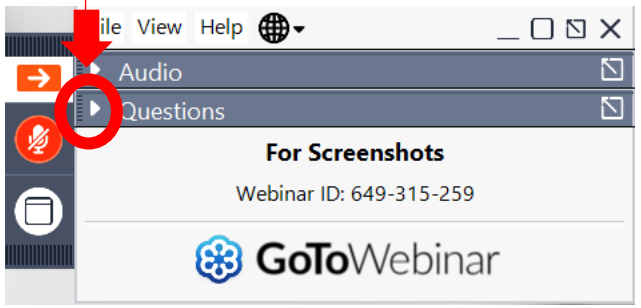
PLEASE

- § 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!

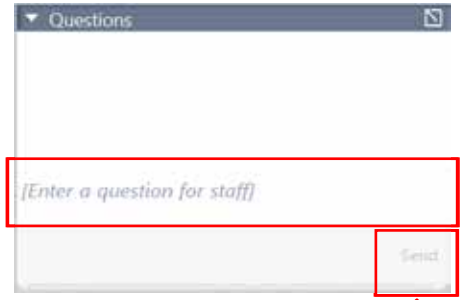
OPENING THE QUESTIONS BOX

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

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.

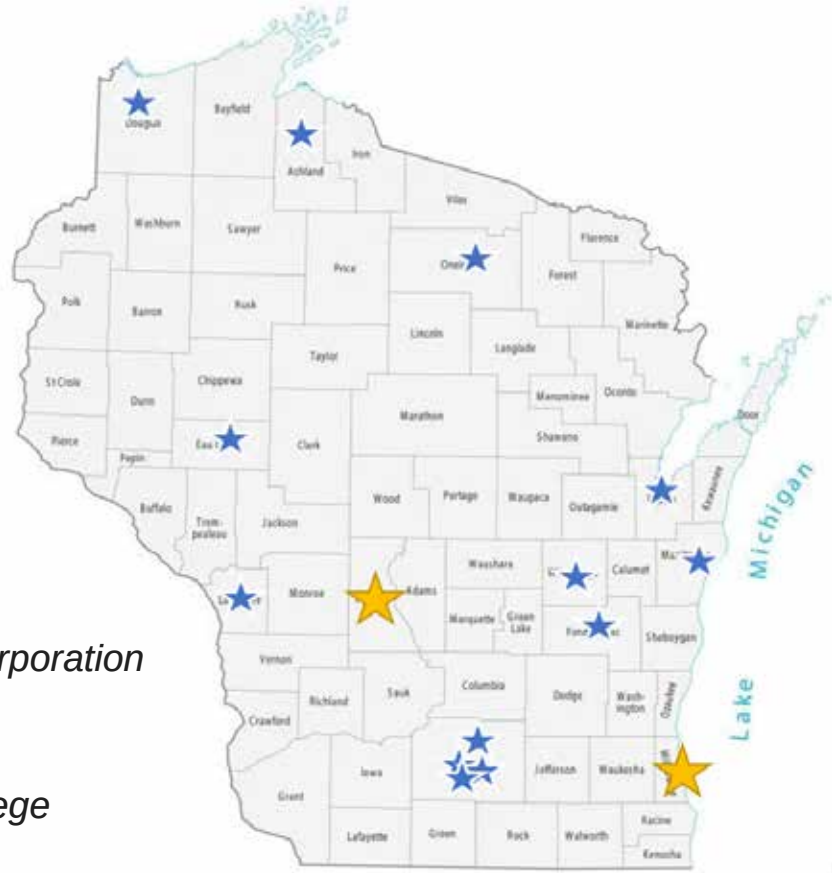
WPI provides services to all of Wisconsin's 72 counties

- 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

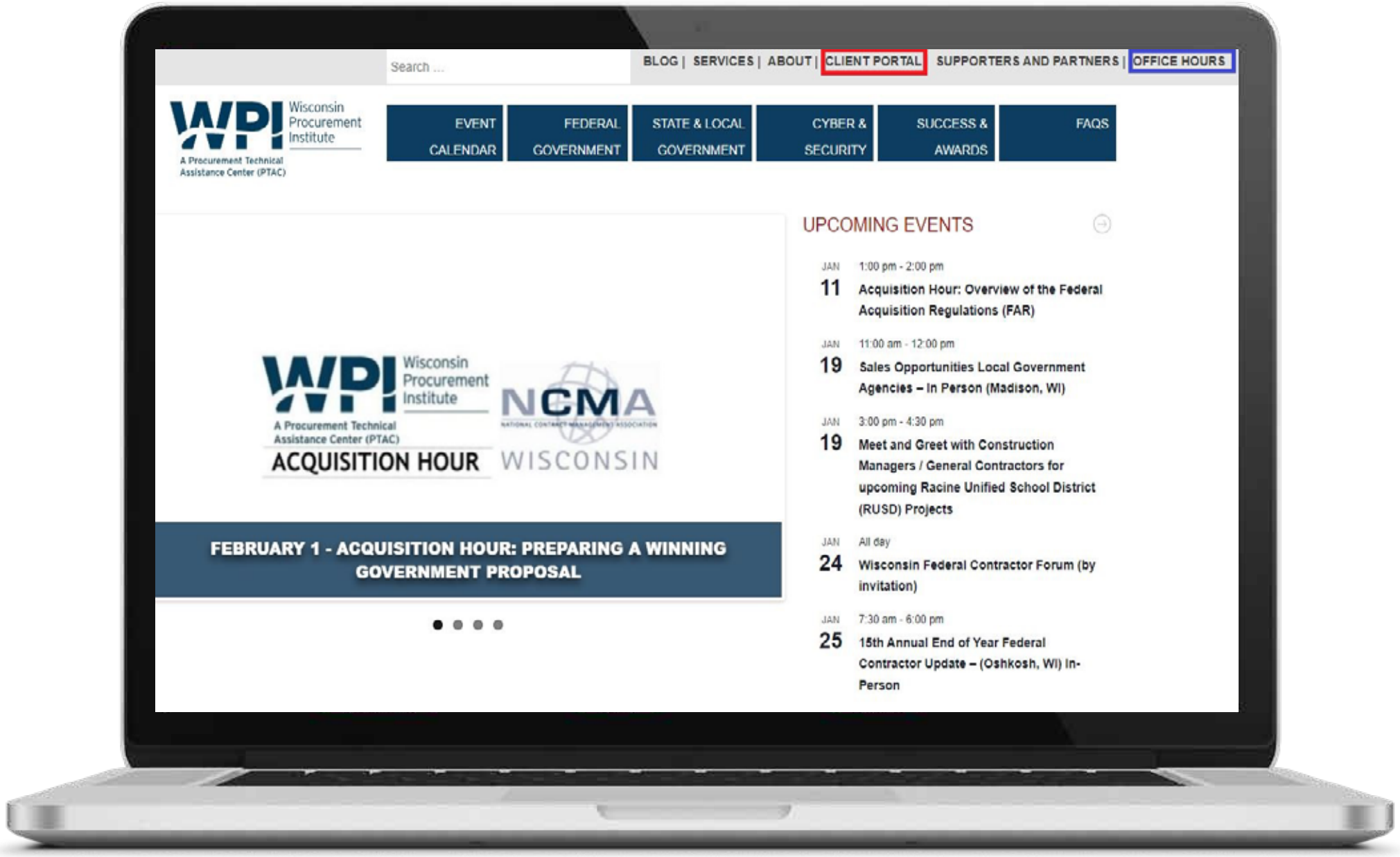
WPI OFFICE LOCATIONS

- **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

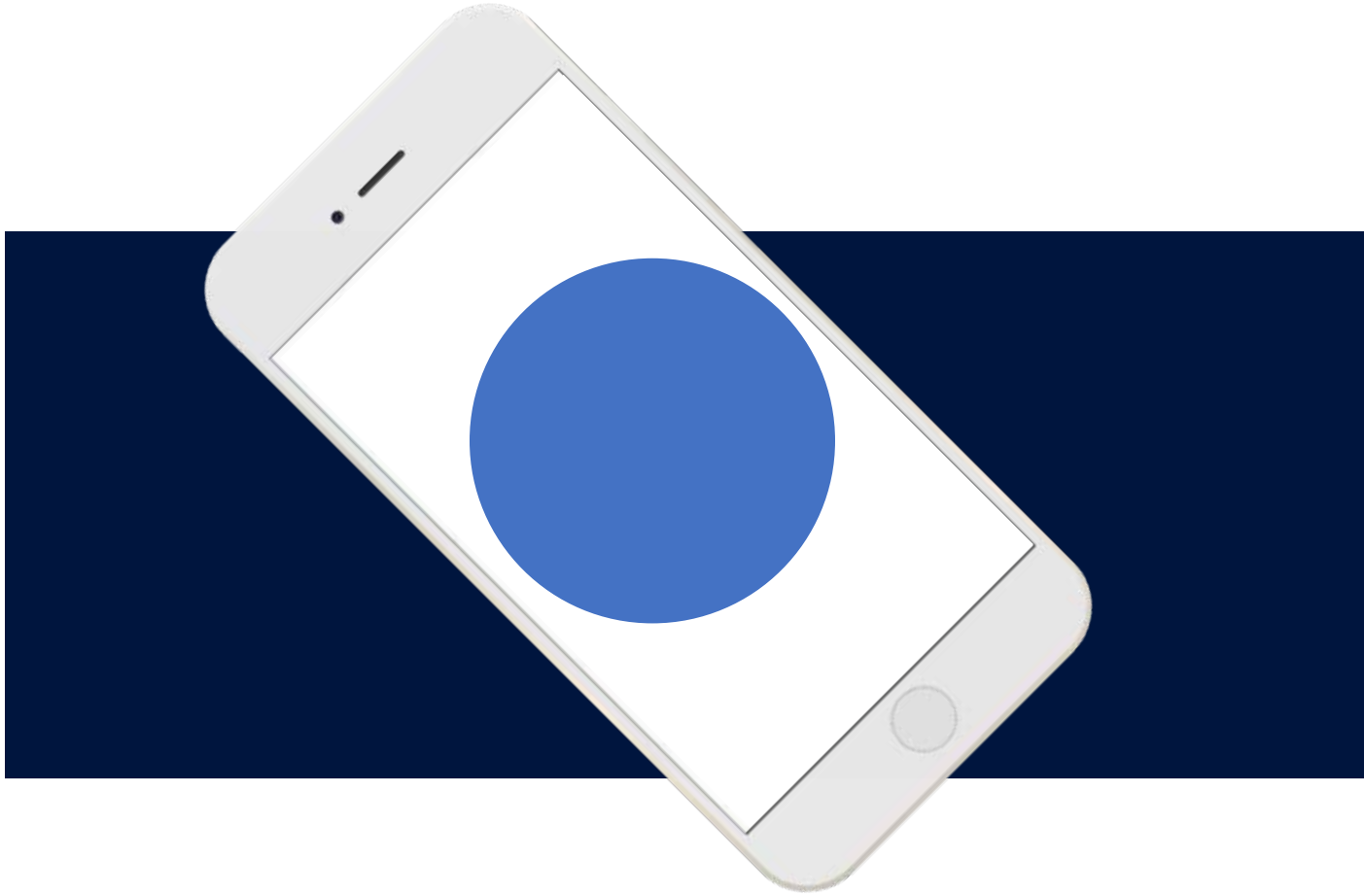
NCMA WISCONSIN


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 – October 20th, 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.

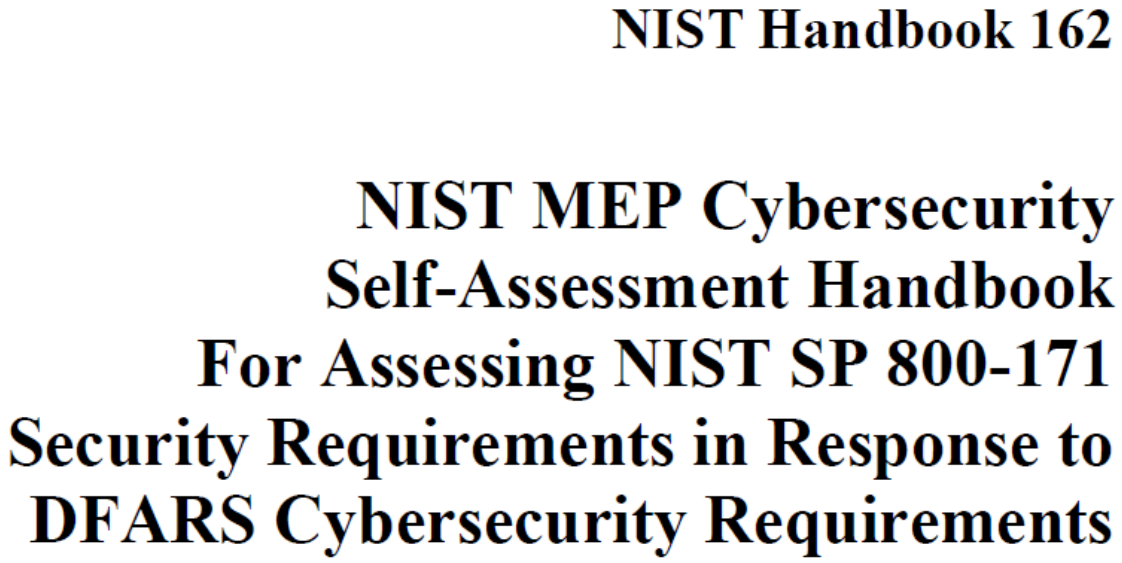
DFARS 252.204-7021

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 800-171r2

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

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	ASSESSMENT OBJECTIVE *Determine if system maintenance is performed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

ASSESSMENT OBJECTIVE

Determine if:

3.7.2[a]	*tools used to conduct system maintenance are controlled.*
3.7.2[b]	*techniques used to conduct system maintenance are controlled.*
3.7.2[c]	*mechanisms used to conduct system maintenance are controlled.*
3.7.2[d]	*personnel used to conduct system maintenance are controlled.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records].

Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Test: [*SELECT FROM:* Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

3.4 Configuration Management

Inventory

Policy

Procedure

Validate

3.8.1	**SECURITY REQUIREMENT** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.8.1[a] *paper media containing CUI is physically controlled.*
	3.8.1[b] *digital media containing CUI is physically controlled.*
	3.8.1[c] *paper media containing CUI is securely stored.*
	3.8.1[d] *digital media containing CUI is securely stored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].

3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	ASSESSMENT OBJECTIVE *Determine if access to CUI on system media is limited to authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection and storage responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

3.4 Configuration Management

Custody

Media Control

Secure Storage

Training

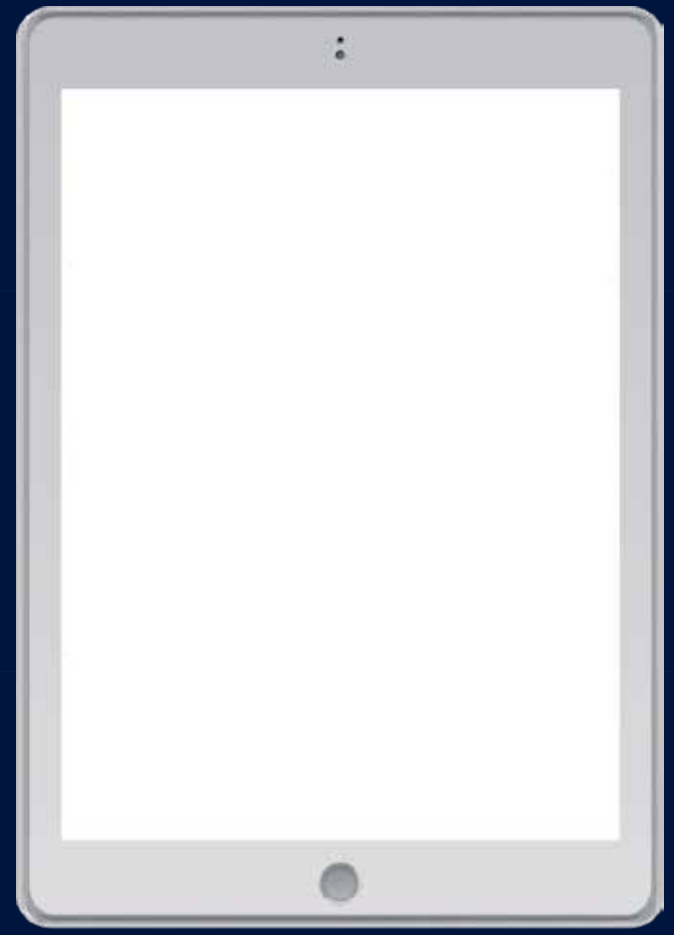
Controls & Objectives

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

Maintenance



Identify and Strategize

- Hardware and Software Inventories
- Patch Window (Schedule)

Process and Procedure

- Document Software / Hardware Baselines and Inventory
- Define IT Policy regarding Maintenance
- Document Processes Thoroughly

Validation

- Perform processes when / how documented
- Create review process to ensure completion

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	ASSESSMENT OBJECTIVE *Determine if system maintenance is performed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

3.7.1 – Meeting the Controls

3.7.1 determine if system maintenance is performed.

Patch Management

Ticket System/Archive

Software Inventory (for asset/tools)

3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

ASSESSMENT OBJECTIVE

Determine if:

3.7.2[a]	*tools used to conduct system maintenance are controlled.*
3.7.2[b]	*techniques used to conduct system maintenance are controlled.*
3.7.2[c]	*mechanisms used to conduct system maintenance are controlled.*
3.7.2[d]	*personnel used to conduct system maintenance are controlled.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records].

Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities].

Test: [*SELECT FROM:* Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

3.7.2 – Meeting the Controls

IT Maintenance Policy

Ticket System/Archive

Software Inventory (for asset/tools)

Visitor Access Policy

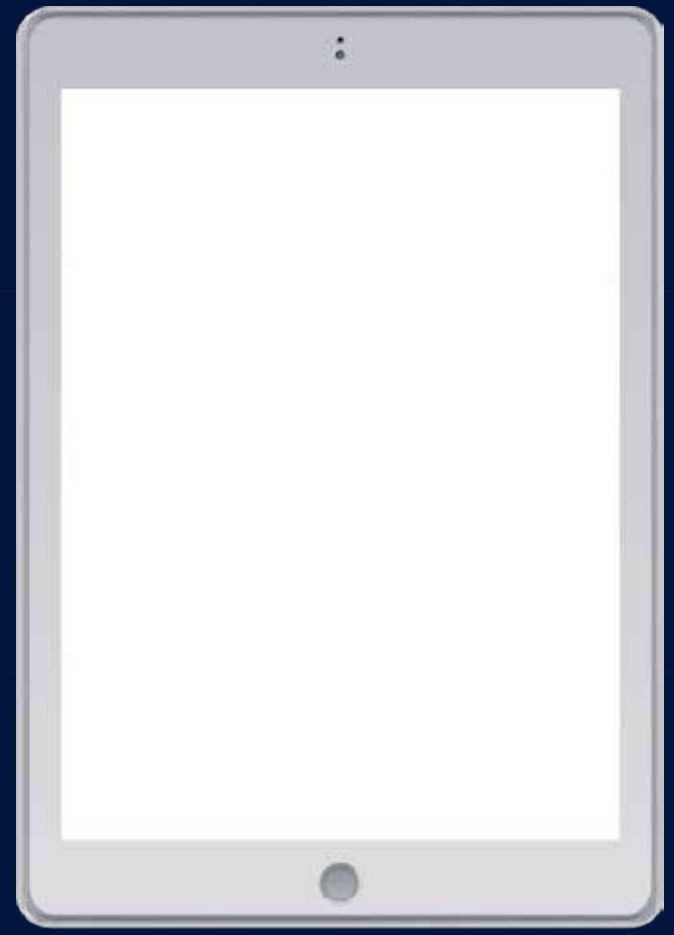
3.7.2[a] tools used to conduct system maintenance are controlled.

3.7.2[b] techniques used to conduct system maintenance are controlled.

3.7.2[c] mechanisms used to condust system maintenance are controlled.

3.7.3[d] personnel used to conduct system maintenance are controlled.

Media Protection



Identify and Strategize

- Media Control Policy
- Appropriate Labels

Process and Procedure

- Media Control Log / Process
- Training and Awareness

Validation

- Media Sanitization Process
- Media Review / Log Review

Configuration Management

3.8.1	**SECURITY REQUIREMENT** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.8.1[a] *paper media containing CUI is physically controlled.*
	3.8.1[b] *digital media containing CUI is physically controlled.*
	3.8.1[c] *paper media containing CUI is securely stored.*
	3.8.1[d] *digital media containing CUI is securely stored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].

3.8.1 – Meeting the Controls

Media Control Policy

Locked Cabinets/Office

Check-Out/Check-In Process

3.8.1[a] paper media containing CUI is physically controlled

3.8.1[b] digital media containing CUI is physically controlled

3.8.1[c] paper media containing CUI is securely stored

3.8.1.[d] digital media containing CUI is securely stored

3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	ASSESSMENT OBJECTIVE *Determine if access to CUI on system media is limited to authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system media protection and storage responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

3.8.2 – Meeting the Controls

Media Control Policy

Locked Cabinets/Office

Check-Out/Check-In Process

Process Review

3.8.2 determine if access to CUI on system media is limited to authorized users

Documentation & Evidence

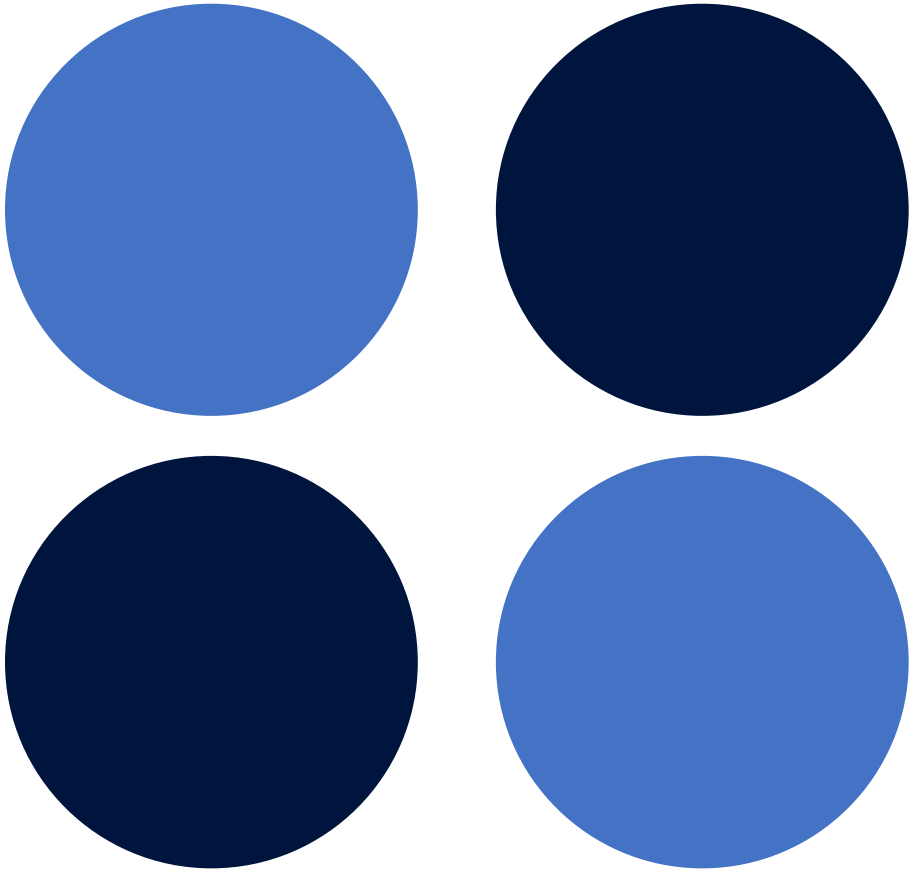
1 — Understanding the Controls

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.

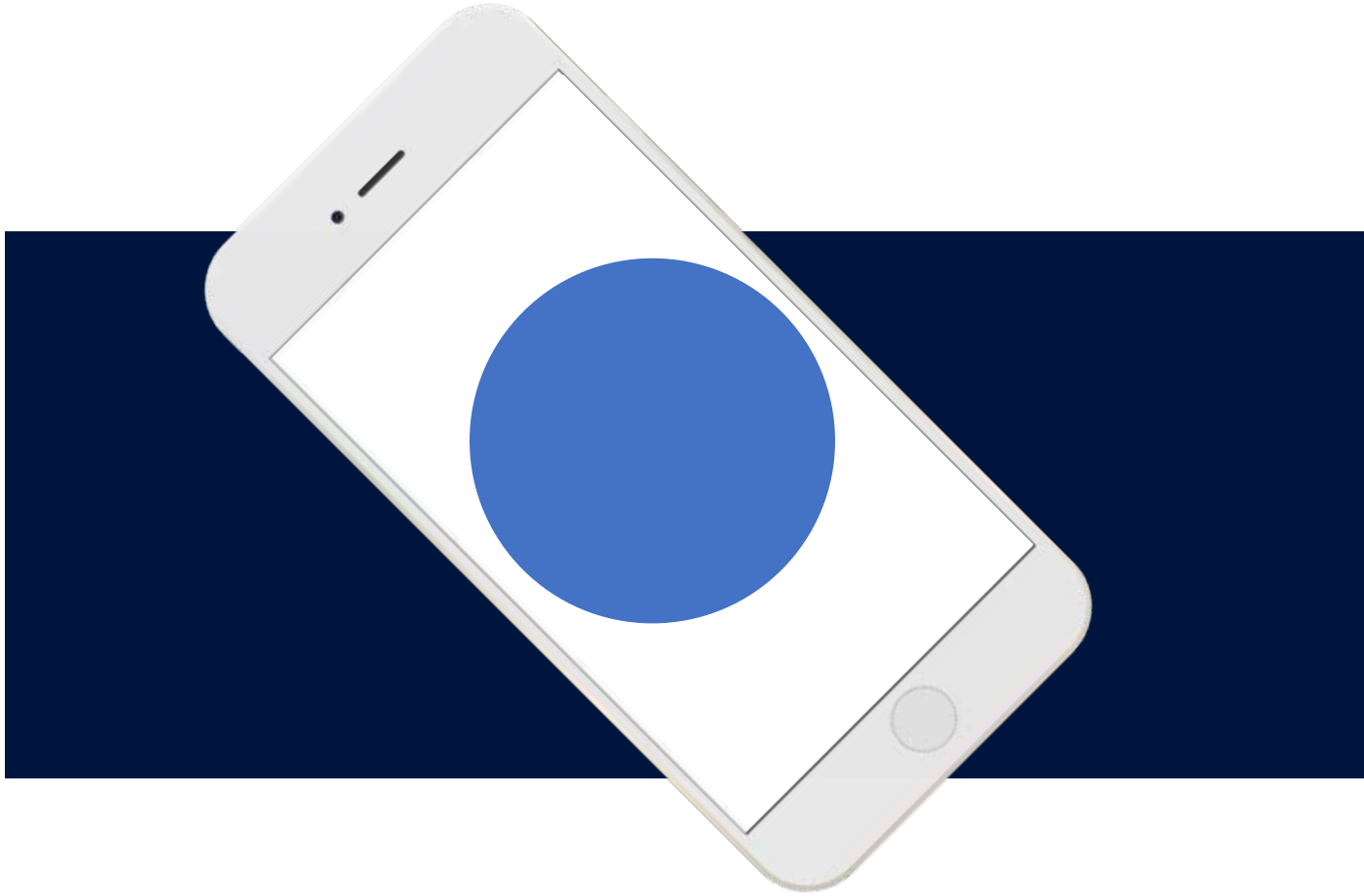
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR

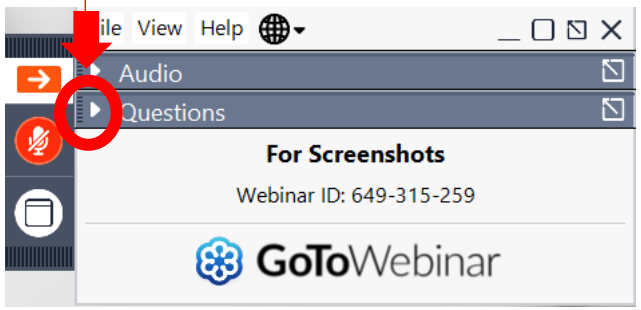


APEX ACCELERATORS

QUESTIONS?

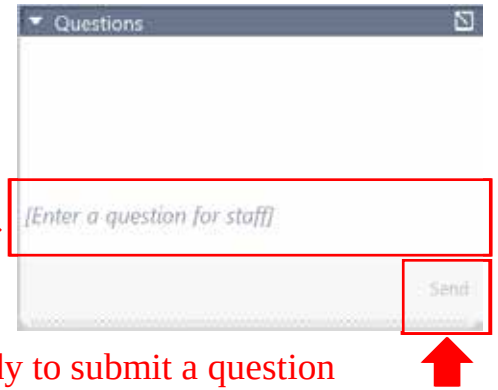
OPENING THE QUESTIONS BOX

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

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
AN APEX ACCELERATOR
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

October 20, 2023

SURVEY

Wisconsin Procurement Institute

October 20, 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