Wisconsin Procurement Institute

APEX ACCELERATORS

# Cyber Friday:

## NIST SP 800.171 – 3.9 Personnel Security and 3.10 Physical Protection

**October 27| 11:00 am - Noon**

**Presented by:**

**Matt Frost, WPI**

NCMA WISCONSIN

# 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

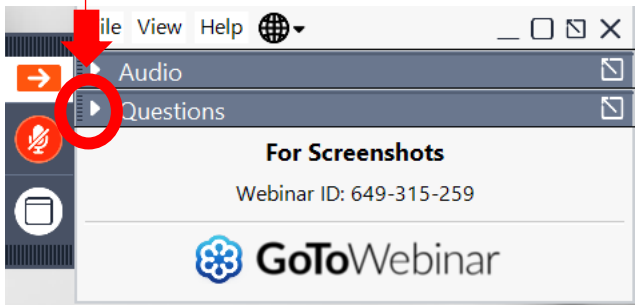
## THANK YOU!

Wisconsin Procurement Institute

NCMA WISCONSIN

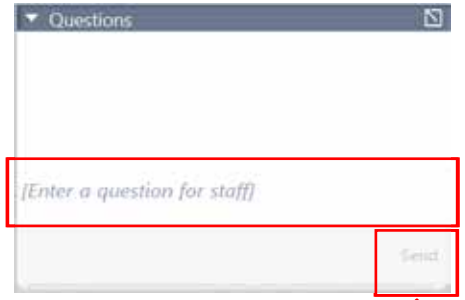
# OPENING THE QUESTIONS BOX

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.

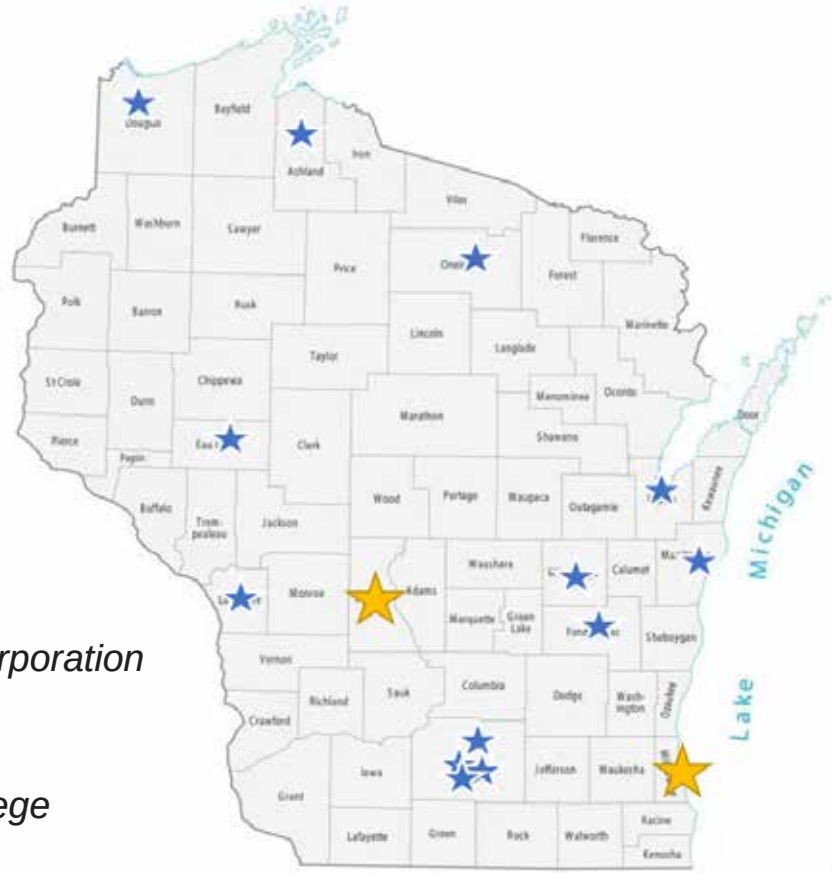
## WPI provides services to all of Wisconsin's 72 counties

- 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

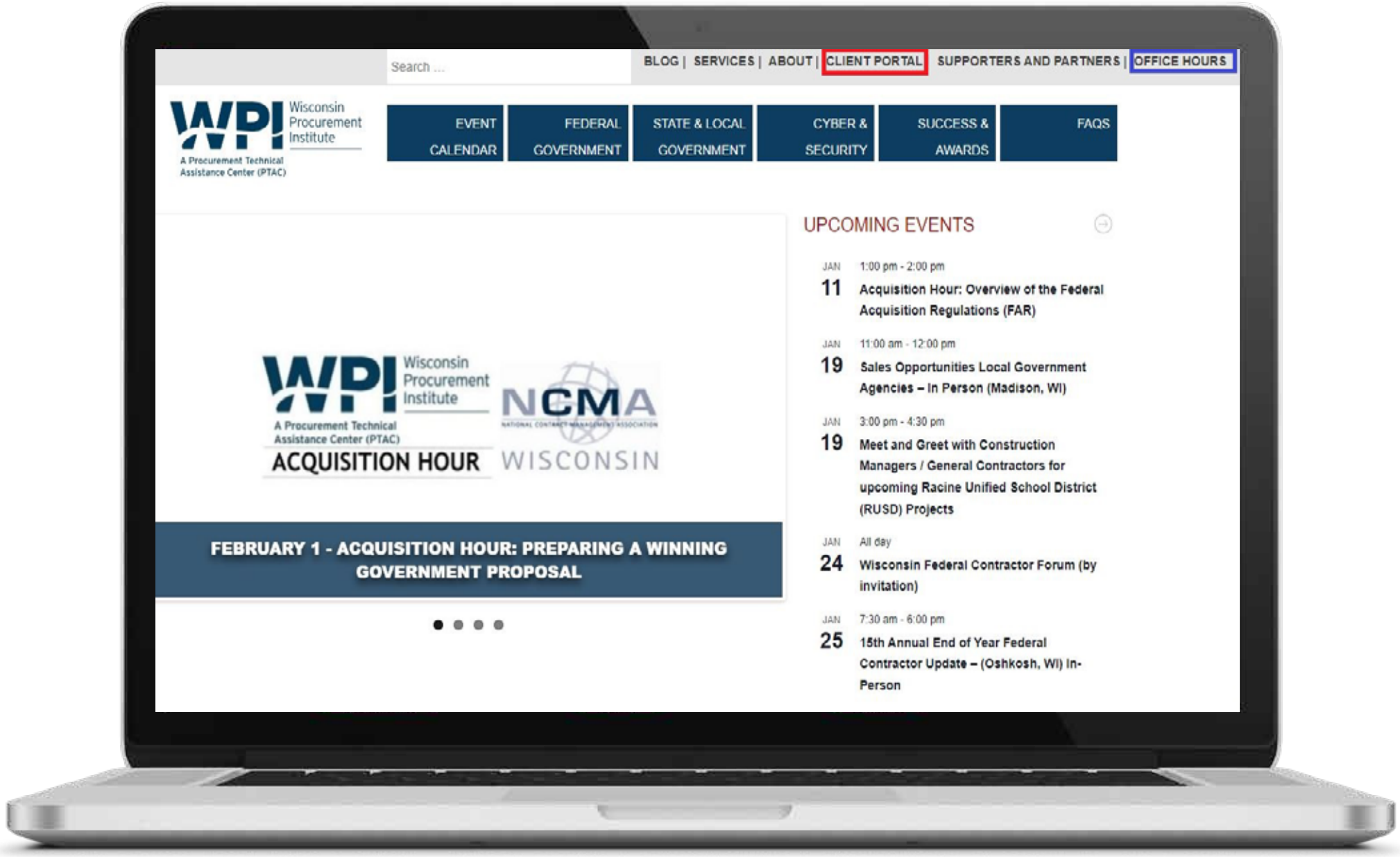
# WPI OFFICE LOCATIONS

- **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



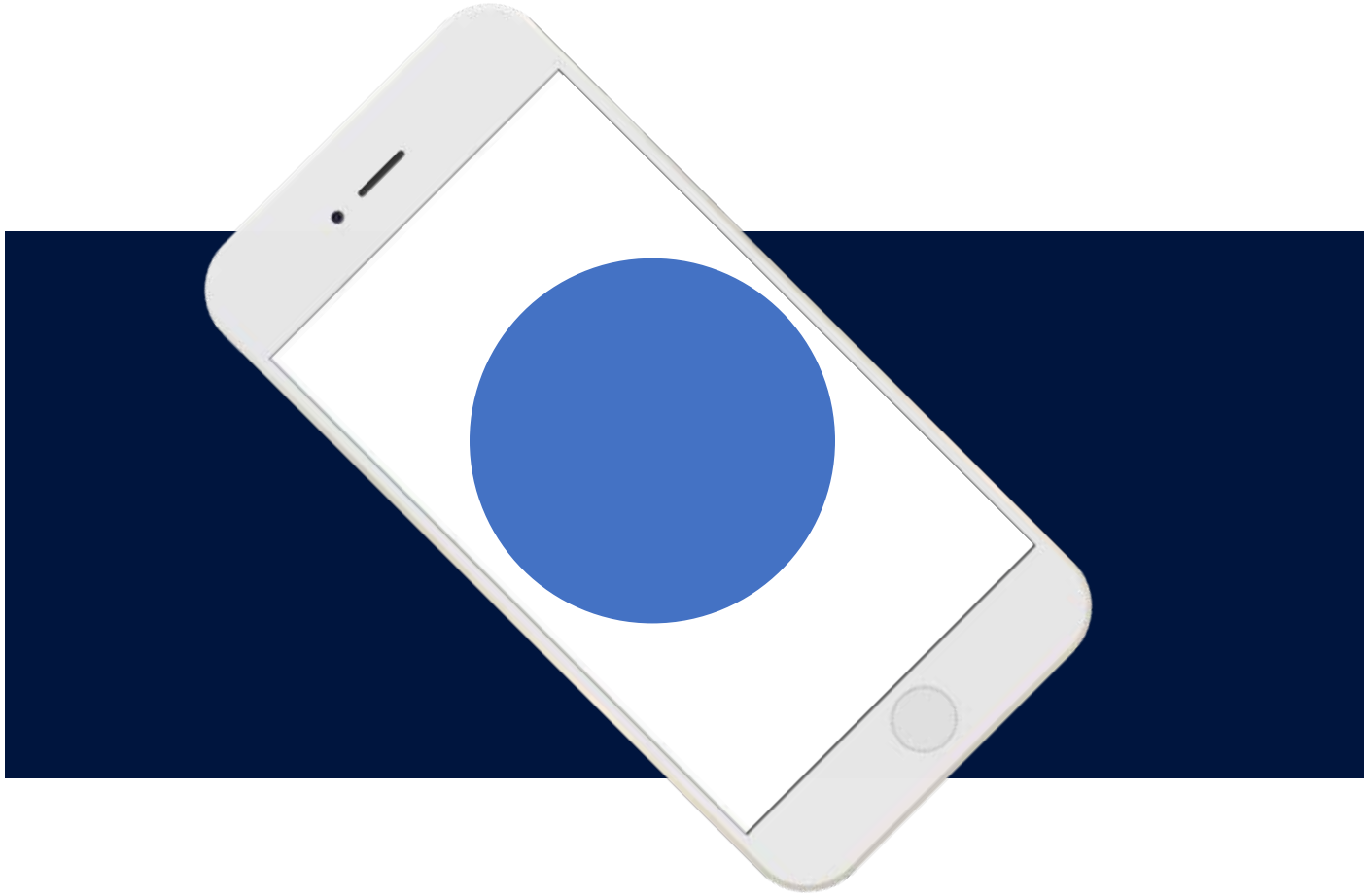

WPI Wisconsin Procurement Institute APEX

NCMA WISCONSIN

# Introduction to NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – October 27th, 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.

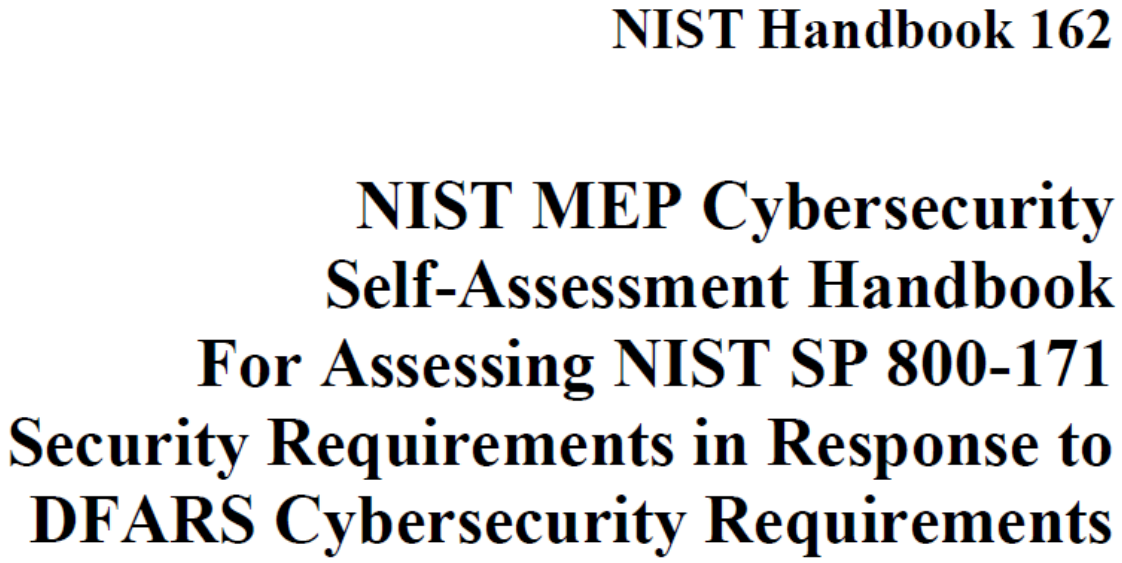
# DFARS 252.204-7021

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

**3.9.1** **Screen individuals prior to authorizing access to organizational systems containing CUI.**

**DISCUSSION**

Personnel security screening (vetting) activities involve the evaluation/assessment of individual's conduct, integrity, judgment, loyalty, reliability, and stability (i.e., the trustworthiness of the individual) prior to authorizing access to organizational systems containing CUI. The screening activities reflect applicable federal laws, Executive Orders, directives, policies, regulations, and specific criteria established for the level of access required for assigned positions.

| 3.9.1 | **SECURITY REQUIREMENT**<br>Screen individuals prior to authorizing access to organizational systems containing CUI. |
|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with personnel security responsibilities; personnel with information security responsibilities].<br>**Test**: [*SELECT FROM:* Organizational processes for personnel screening]. |

# 3.9 Personnel Security

Due Dillegence

Provision

Offboard

Validate

**3.10.1** **Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.**

**DISCUSSION**

This requirement applies to employees, individuals with permanent physical access authorization credentials, and visitors. Authorized individuals have credentials that include badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed consistent with applicable laws, directives, policies, regulations, standards, procedures, and guidelines. This requirement applies only to areas within facilities that have not been designated as publicly accessible.

Limiting physical access to equipment may include placing equipment in locked rooms or other secured areas and allowing access to authorized individuals only; and placing equipment in locations that can be monitored by organizational personnel. Computing devices, external disk drives, networking devices, monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of equipment.

| 3.10.1 | **SECURITY REQUIREMENT**<br>Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. |
|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* |
| | **3.10.1[a]** *authorized individuals allowed physical access are identified.* |
| | **3.10.1[b]** *physical access to organizational systems is limited to authorized individuals.* |
| | **3.10.1[c]** *physical access to equipment is limited to authorized individuals.* |
| | **3.10.1[d]** *physical access to operating environments is limited to authorized individuals.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records].<br>**Interview:** [*SELECT FROM:* Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities].<br>**Test:** [*SELECT FROM:* Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations]. |

# 3.10 Physical Security

Authorize

Secure

Restrict

Record

# Controls & Objectives

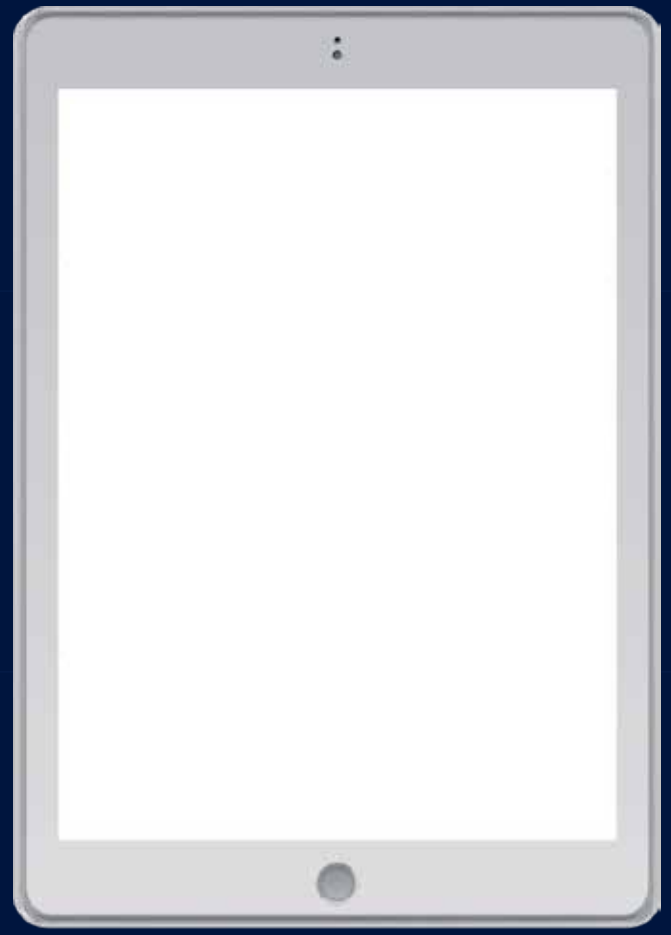


1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

# Physical Security



## Onboarding Process

- Screen / Interview / Information Gather
- Consider Risks of Role to Company
- Follow Process / Policy
- Save Records

## Offboard Process

- Determination of Exit / Reason Clearly Stated
- Follow Process. / Policy
- Remove Permissions / Access
- Save Records

| 3.9.1 | **SECURITY REQUIREMENT**<br>Screen individuals prior to authorizing access to organizational systems containing CUI. |
|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel screening; records of screened personnel; system security plan; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with personnel security responsibilities; personnel with information security responsibilities].<br>**Test**: [*SELECT FROM:* Organizational processes for personnel screening]. |

# 3.9.1 – Meeting the Controls

## ONBOARDING PROCESS

**3.9.1 Determine if individuals are screened prior to authorizing access to organizational systems containing CUI.**

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

Include formal authorization of employee access.

| 3.9.2 | **SECURITY REQUIREMENT**<br>Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. |
|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* |
| | **3.9.2[a]** *a policy and/or process for terminating system access and any credentials coincident with personnel actions is established.* |
| | **3.9.2[b]** *system access and credentials are terminated consistent with personnel actions such as termination or transfer.* |
| | **3.9.2[c]** *the system is protected during and after personnel transfer actions.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Personnel security policy; procedures addressing personnel transfer and termination; records of personnel transfer and termination actions; list of system accounts; records of terminated or revoked authenticators and credentials; records of exit interviews; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with personnel security responsibilities; personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].<br>**Test**: [*SELECT FROM:* Organizational processes for personnel transfer and termination; mechanisms supporting or implementing personnel transfer and termination notifications; mechanisms for disabling system access and revoking authenticators]. |

# 3.9.2 – Meeting the Controls

## OFFBOARDING PROCESS

**3.9.2[a] A policy and / or process for terminating system access and any credentials coincident with personnel actions is established.**

## VALIDATE ACCESS REMOVAL

**3.9.2[b] System access and credentials are terminated consistent with personnel actions such as termination or transfer.**

**3.9.2[c] The system is protected during and after personnel transfer actions**

# Physical Protection

## Identification and Authorization

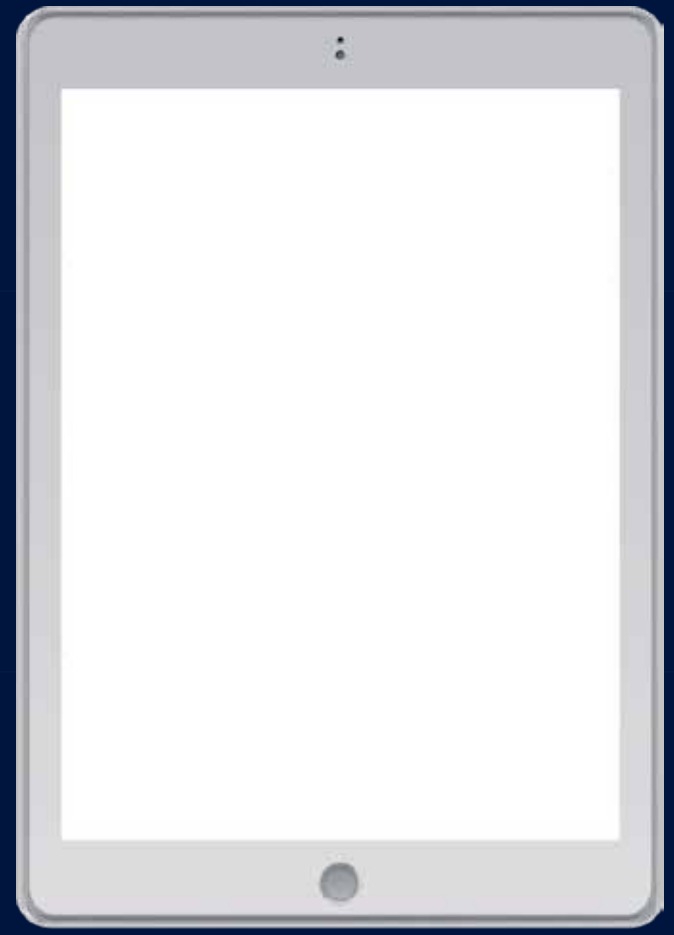
- Users Are Authorized and Identifiable
- Records of Process are Accurate and Available
- Visitors are clearly identified

## Observe and Monitor

- Badges for Visitors
- Escorting Procedures and Briefings
- Training and Process

## Validate and Record Keeping

- Visitor Log Creation and Retention
- Training Records and Retention



| 3.10.1 | **SECURITY REQUIREMENT**<br>Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. |
|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* |
| | **3.10.1[a]** *authorized individuals allowed physical access are identified.* |
| | **3.10.1[b]** *physical access to organizational systems is limited to authorized individuals.* |
| | **3.10.1[c]** *physical access to equipment is limited to authorized individuals.* |
| | **3.10.1[d]** *physical access to operating environments is limited to authorized individuals.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records].<br>**Interview:** [*SELECT FROM:* Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities].<br>**Test:** [*SELECT FROM:* Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations]. |

# 3.10.1 – Meeting the Controls

ONBOARDING

VISITOR SIGN IN

**3.10.1[a] authorized individuals allowed physical access are identified.**

ENTRY CONTROL

ESCORT POLICY

**3.10.1[b] physical access to organizational systems is limited to authorized individuals.**

**3.10.1[c] physical access to equipment is limited to authorized individuals.**

**3.10.1[d] physical access to operating environments is limited to authorized individuals.**

| 3.10.2 | **SECURITY REQUIREMENT**<br>Protect and monitor the physical facility and support infrastructure for organizational systems. |
|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* |
| | **3.10.2[a]** *the physical facility where organizational systems reside is protected.* |
| | **3.10.2[b]** *the support infrastructure for organizational systems is protected.* |
| | **3.10.2[c]** *the physical facility where organizational systems reside is monitored.* |
| | **3.10.2[d]** *the support infrastructure for organizational systems is monitored.* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine:** [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access monitoring; system security plan; physical access logs or records; physical access monitoring records; physical access log reviews; other relevant documents or records].<br>**Interview:** [*SELECT FROM:* Personnel with physical access monitoring responsibilities; personnel with incident response responsibilities; personnel with information security responsibilities].<br>**Test:** [*SELECT FROM:* Organizational processes for monitoring physical access; mechanisms supporting or implementing physical access monitoring; mechanisms supporting or implementing the review of physical access logs]. |

# 3.10.2 – Meeting the Controls

## SECURITY POLICY

**3.10.2[a] the physical facility where organizational systems reside is protected.**

**3.10.2[b] the support infrastructure for organizational systems is protected.**

## ESCORT & SECURITY POLICY

**3.10.2[c] the physical facility where organizational systems reside is monitored.**

**3.10.2[d] the support infrastructure for organizational systems is monitored.**

# 3.10 Physical Security Policy Highlights

**Visitor Logging/ Escorting**

**Security Features**

**Security Processes**

**Records And Training**

# Documentation & Evidence



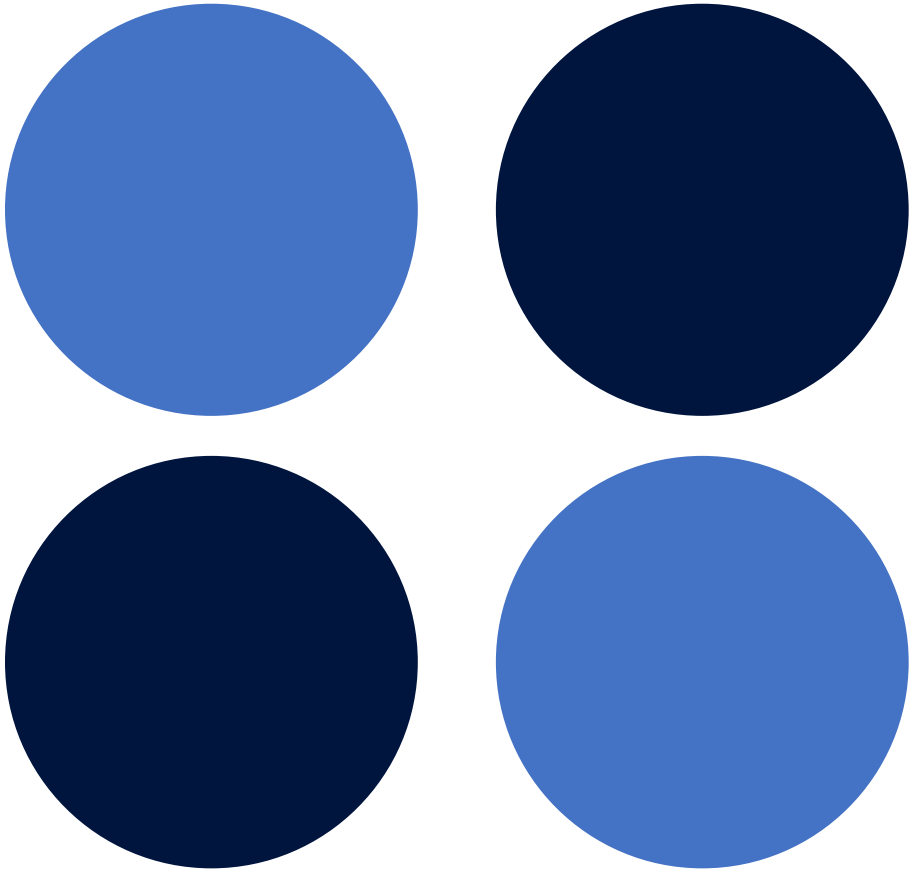
1 Understanding the Controls

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.

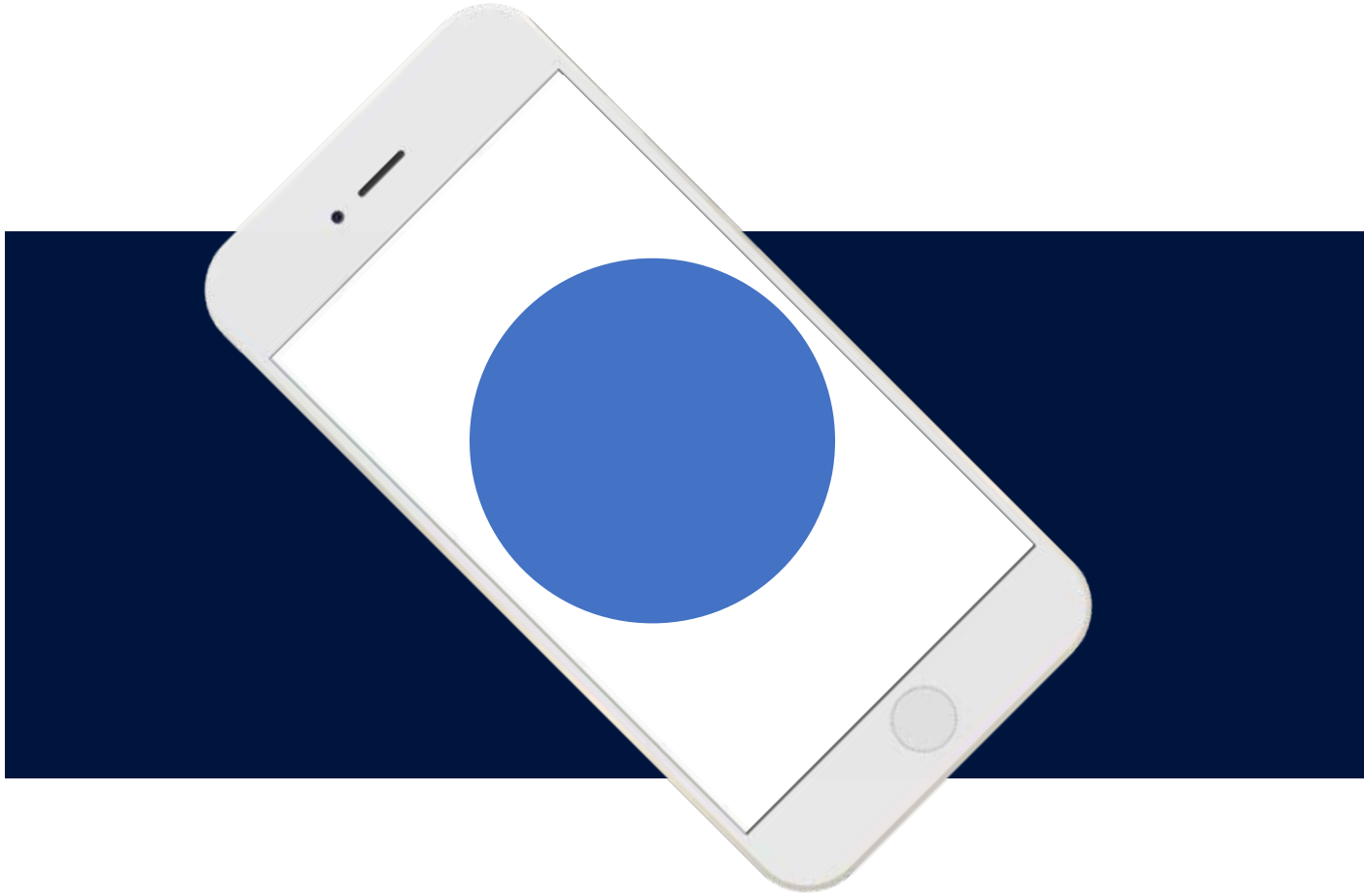
**Reviews**
are periodically conducted, tracked, and summarized.

**Matthew Frost**

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR

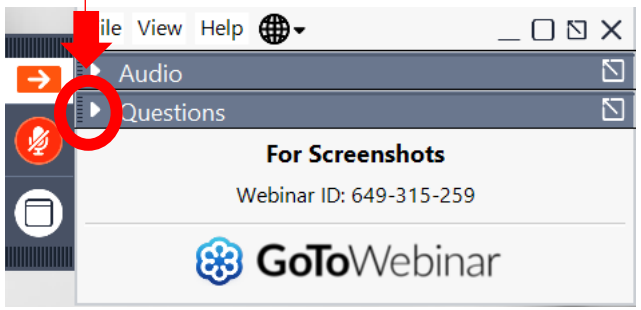


APEX ACCELERATORS

# QUESTIONS?

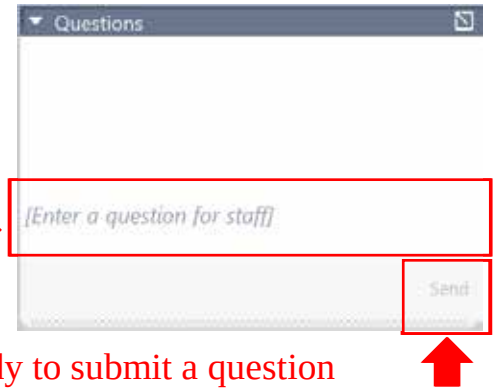
## OPENING THE QUESTIONS BOX

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
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*

**October 27, 2023**

# SURVEY

Wisconsin Procurement Institute

October 27, 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