Wisconsin Procurement Institute
AN APEX ACCELERATOR

APEX ACCELERATORS

Cyber Friday:
NIST SP 800.171 – 3.6 Incident Response

October 6 | 11:00 am – Noon
Presented by Matt Frost, WPI

Wisconsin Procurement Institute
Cyber Friday

Webinar Etiquette

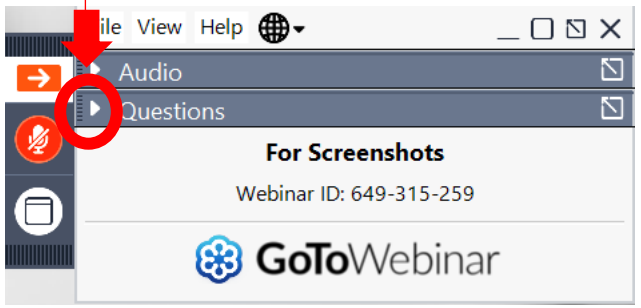
PLEASE

- § 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!

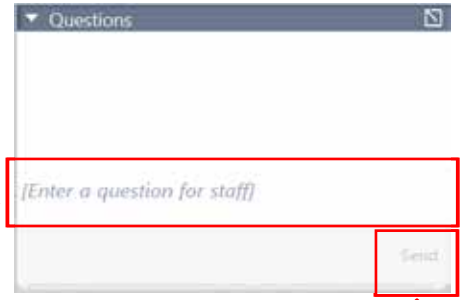
OPENING THE QUESTIONS BOX

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.

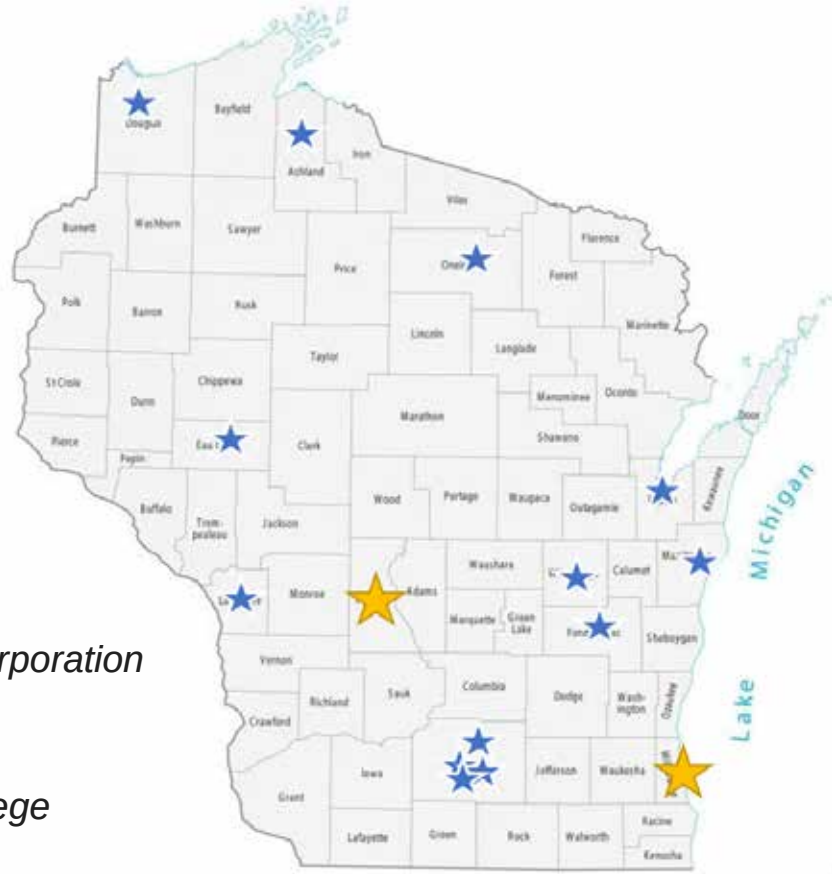
WPI provides services to all of Wisconsin's 72 counties

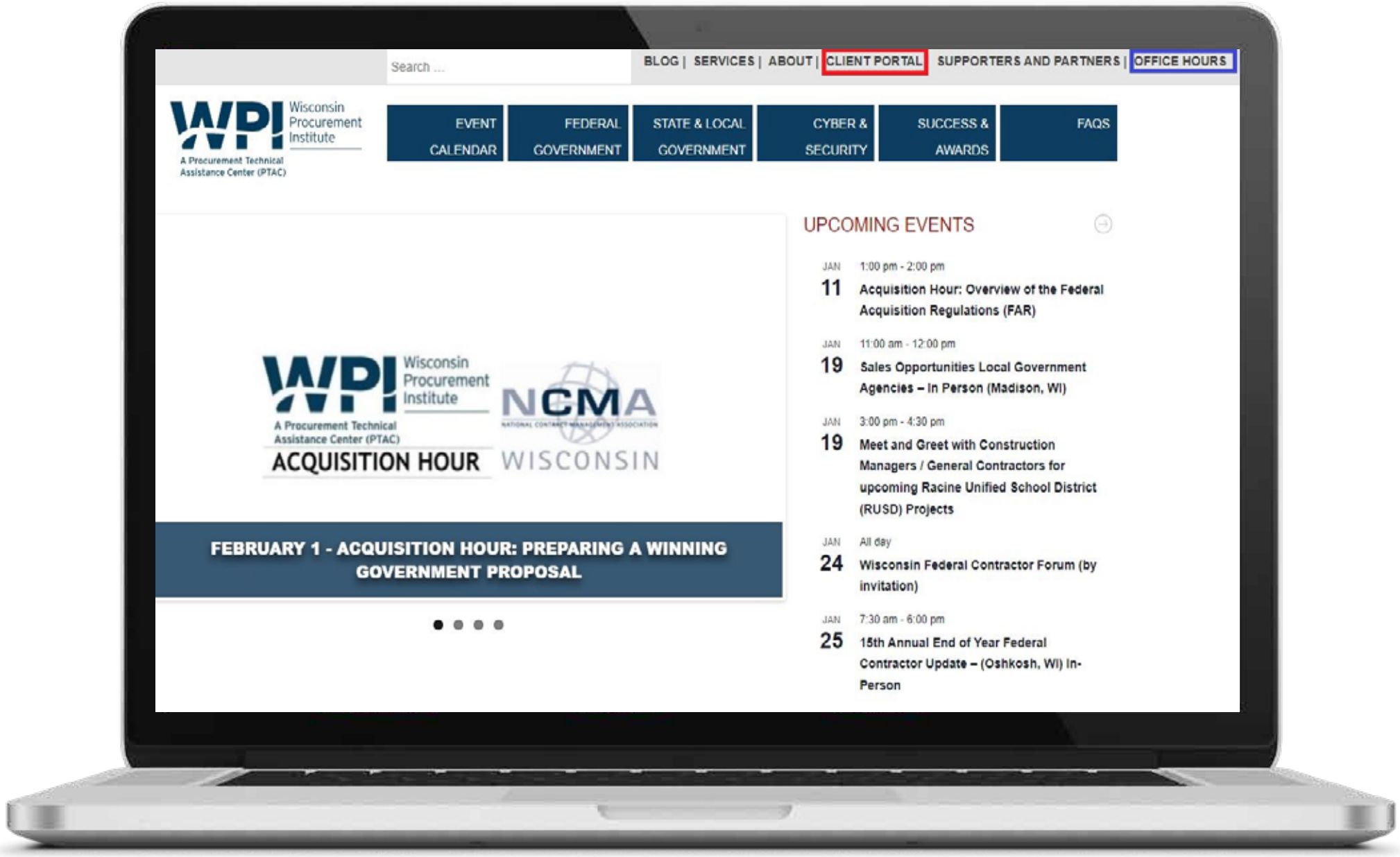
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops
- Conferences including one on one buyer meetings – Marketplace, The Contracting Academy, Small Business Academy, Wisconsin Federal Contractor Forum, Acquisition Hour, Cyber Fridays,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

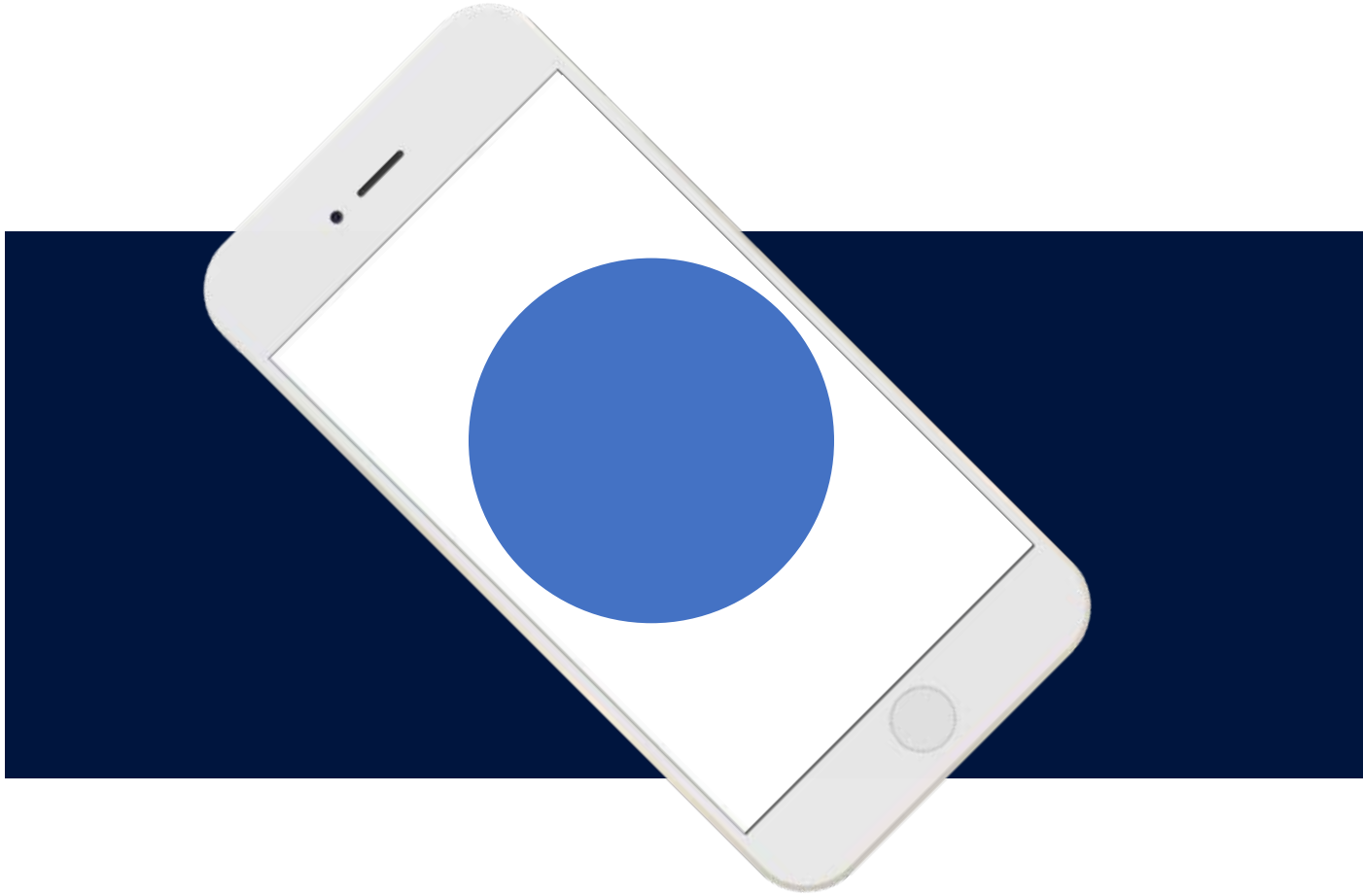



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL | SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
Wisconsin Procurement Institute
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 – October 6th, 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

NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

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

NIST SP 800-171

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

Incident Response Plan

- Statement of Management Commitment
- Purpose and Objectives
- Scope of Policy
- Organizational Structure (Roles and Responsibilities)
- Prioritization or Severity Ratings of Incidents
- Performance Measures (Milestones)
- Reporting and Contact

PURPOSE & OBJECTIVES

Purpose

Outline the purpose of the incident response plan. List the plan's goals and objectives. Explain why this document has been created and what you hope to achieve with it.

For example:

The purpose of this document is to provide effective emergency response methods that will ensure the well-being of all employees and/or visitors of [Company Name]. This document will establish an effective incident response framework. It will also explain how to communicate the incident quickly and clearly to key stakeholders and how to minimize disruption to the working environment.

OR

The purpose of this document is to describe the plan for responding to information security incidents at [Company Name]. This document will explain how to detect and react to cybersecurity incidents and data breaches, determine their scope and risk, respond appropriately and quickly, and communicate the results and risks to all stakeholders.

Incident Response Team

Management

- Ownership and Authority
- Leadership and Delegation
- Accountability

IT Team Leader

- Technical Response
- Translating Concerns and Solutions
- Change Log and Incident Journal
- Forensic Assistance

Operations

- Business Continuity
- Customer Concern Response
- Incident Intelligence

Marketing & Legal

- Customer Communications
- Reporting Requirements
- Public Statements
- Liason with Law Enforcement

3.6.1 **Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.**

DISCUSSION

Organizations recognize that incident handling capability is dependent on the capabilities of organizational systems and the mission/business processes being supported by those systems. Organizations consider incident handling as part of the definition, design, and development of mission/business processes and systems. Incident-related information can be obtained from a variety of sources including audit monitoring, network monitoring, physical access monitoring, user and administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including mission/business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive.

As part of user response activities, incident response training is provided by organizations and is linked directly to the assigned roles and responsibilities of organizational personnel to ensure that the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the system; system administrators may require additional training on how to handle or remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification/reporting of suspicious activities from external and internal sources. User response activities also includes incident response assistance which may consist of help desk support, assistance groups, and access to forensics services or consumer redress services, when required.

3.6.1	**SECURITY REQUIREMENT** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.6.1[a] *an operational incident-handling capability is established.*
	3.6.1[b] *the operational incident-handling capability includes preparation.*
	3.6.1[c] *the operational incident-handling capability includes detection.*
	3.6.1[d] *the operational incident-handling capability includes analysis.*
	3.6.1[e] *the operational incident-handling capability includes containment.*
	3.6.1[f] *the operational incident-handling capability includes recovery.*
	3.6.1[g] *the operational incident-handling capability includes user response activities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Incident response policy; contingency planning policy; procedures addressing incident handling; procedures addressing incident response assistance; incident response plan; contingency plan; system security plan; procedures addressing incident response training; incident response training curriculum; incident response training materials; incident response training records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with incident handling responsibilities; personnel with contingency planning responsibilities; personnel with incident response training and operational responsibilities; personnel with incident response assistance and support responsibilities; personnel with access to incident response support and assistance capability; personnel with information security responsibilities]. Test: [*SELECT FROM:* Incident-handling capability for the organization; organizational processes for incident response assistance; mechanisms supporting or implementing incident response assistance].

3.6.2	SECURITY REQUIREMENT Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.6.2[a]	*incidents are tracked.*
	3.6.2[b]	*incidents are documented.*
	3.6.2[c]	*authorities to whom incidents are to be reported are identified.*
	3.6.2[d]	*organizational officials to whom incidents are to be reported are identified.*
	3.6.2[e]	*identified authorities are notified of incidents.*
	3.6.2[f]	*identified organizational officials are notified of incidents.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	

3.6.3	SECURITY REQUIREMENT Test the organizational incident response capability.
	ASSESSMENT OBJECTIVE *Determine if the incident response capability is tested.*

Controls & Objectives

NIST SP 800-171

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

3.6.1	SECURITY REQUIREMENT Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.6.1[a]	*an operational incident-handling capability is established.*
	3.6.1[b]	*the operational incident-handling capability includes preparation.*
	3.6.1[c]	*the operational incident-handling capability includes detection.*
	3.6.1[d]	*the operational incident-handling capability includes analysis.*
	3.6.1[e]	*the operational incident-handling capability includes containment.*
	3.6.1[f]	*the operational incident-handling capability includes recovery.*
	3.6.1[g]	*the operational incident-handling capability includes user response activities.*

3.6.1– Meeting the Controls

TABLE OF CONTENTS

Incident Response

3.6.2	**SECURITY REQUIREMENT** Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.6.2[a]	*incidents are tracked.*
	3.6.2[b]	*incidents are documented.*
	3.6.2[c]	*authorities to whom incidents are to be reported are identified.*
	3.6.2[d]	*organizational officials to whom incidents are to be reported are identified.*
	3.6.2[e]	*identified authorities are notified of incidents.*
	3.6.2[f]	*identified organizational officials are notified of incidents.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	

3.6.2 – Meeting The Controls

Incident Response Recording	
Incident Identification	• Record the date and time of the incident's discovery. • Document the source or method of detection (e.g., security alert, user report, system log). • Specify the affected systems, networks, or applications.
Incident Classification	• Document the nature and type of the incident (e.g., malware infection, unauthorized access). • Record the potential impact on critical assets, data, and operations. • Note the initial steps taken for containment and isolation. • Classify the incident severity (e.g., low, moderate, high) based on impact and threat level. • Specify the incident category (e.g., data breach, DDoS attack, insider threat).
Response Actions	• Document all actions taken to contain and mitigate the incident. • Record changes made to affected systems or configurations. • Specify tools, techniques, and procedures used for analysis and containment.
Communication Log	• Maintain a log of all internal and external communications related to the incident. • Document communication timestamps, recipients, and content discussed. • Note decisions made during communication with stakeholders. In the event these communications exist in digital record (such as email), please catalogue time and means of exchange for their reference.

3.6.2 – Meeting The Controls

Impact Assessment	• Document the extent of data or system compromise. • Record potential legal, financial, and reputational impacts. • Note the potential impact on stakeholders, customers, and partners.
Containment and Eradication	• Document the steps taken to contain the incident and prevent further spread. • Record actions to eradicate malware, close vulnerabilities, and remove unauthorized access. • Specify changes made to network configurations or access permissions.
Recovery Procedures	• Document the restoration process for affected systems and data. • Record validation steps to ensure systems are free from malware or vulnerabilities. • Note any additional security measures implemented post-incident.
Post-Incident Analysis	• Document lessons learned from the incident response process. • Record recommendations for improving incident response procedures. • Specify areas of the organization that require security awareness training or policy updates based on incident findings.
Reporting/Closure	• Document the resolution of the incident and the restoration of normal operations. • Prepare a detailed incident report outlining the incident, response actions, and lessons learned. • Specify any follow-up actions required and their respective deadlines.

Incident Response

3.6.3	**SECURITY REQUIREMENT** Test the organizational incident response capability.
	ASSESSMENT OBJECTIVE *Determine if the incident response capability is tested.*

Documentation & Evidence

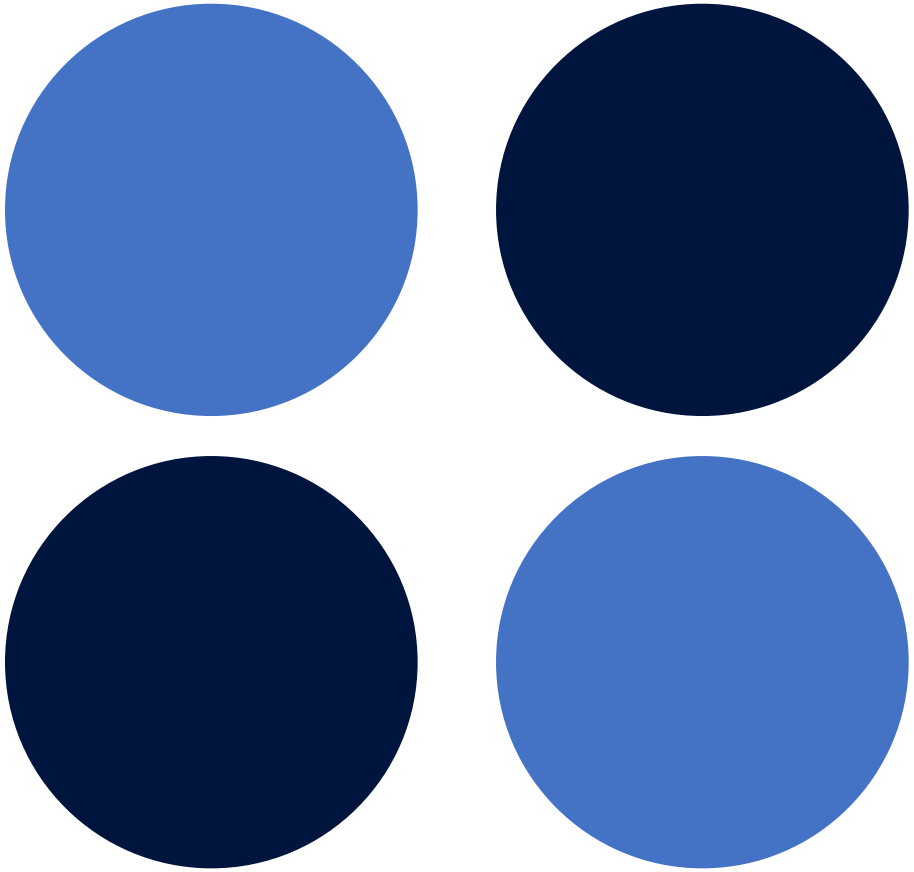
1 — Understanding the Controls

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.

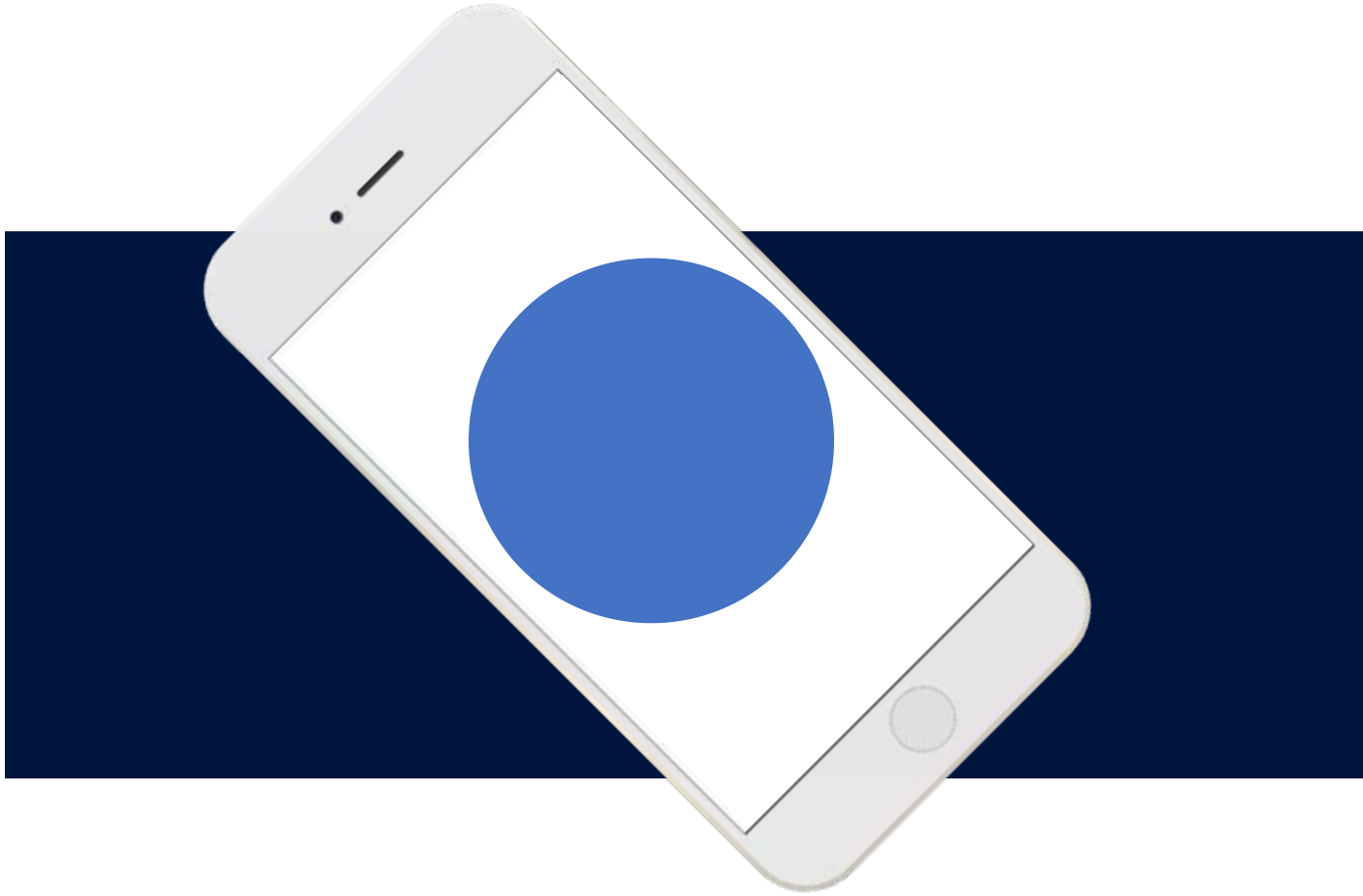
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR

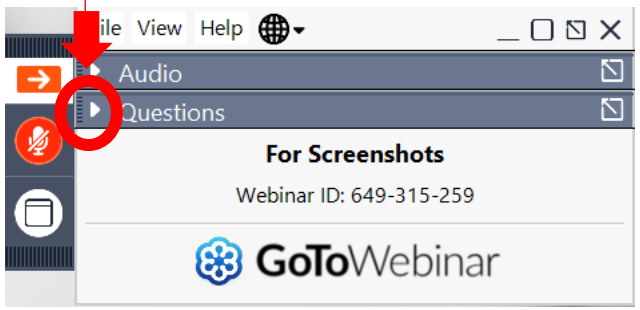


APEX ACCELERATORS

QUESTIONS?

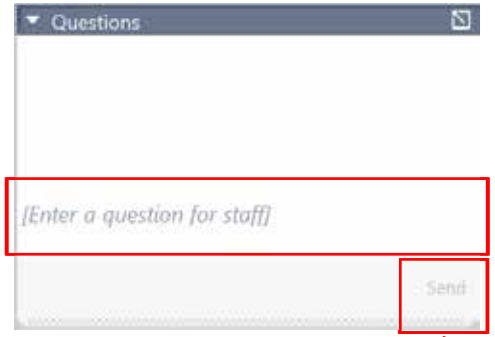
OPENING THE QUESTIONS BOX

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

CYBER FRIDAY LIVE WEBINAR SERIES

- 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)

October 6, 2023

SURVEY

Wisconsin Procurement Institute
AN APEX ACCELERATOR

October 6, 2023

APEX ACCELERATORS

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