Wisconsin Procurement Institute

AN APEX ACCELERATOR

APEX ACCELERATORS

CYBER FRIDAY:

Preparing For a Cyber Incident

March 10, 2023 @ 11:00 am - Noon

Presented by Matt Frost, WPI

Wisconsin Procurement Institute

AN APEX ACCELERATOR

Cyber Friday

Webinar Etiquette

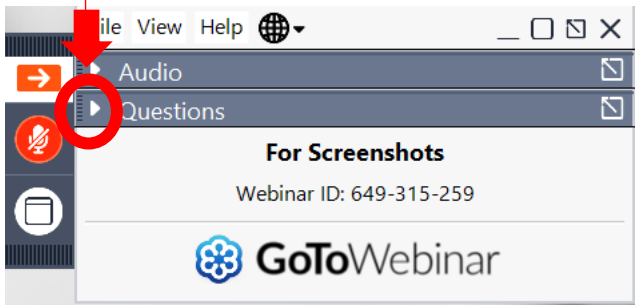
PLEASE

- 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!

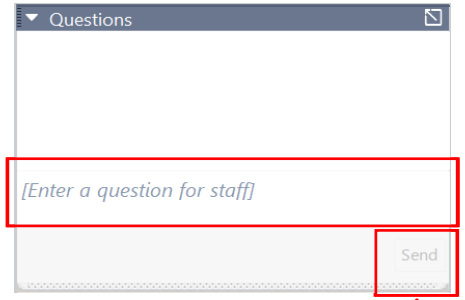
OPENING THE QUESTIONS BOX

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 ACCELERATOR

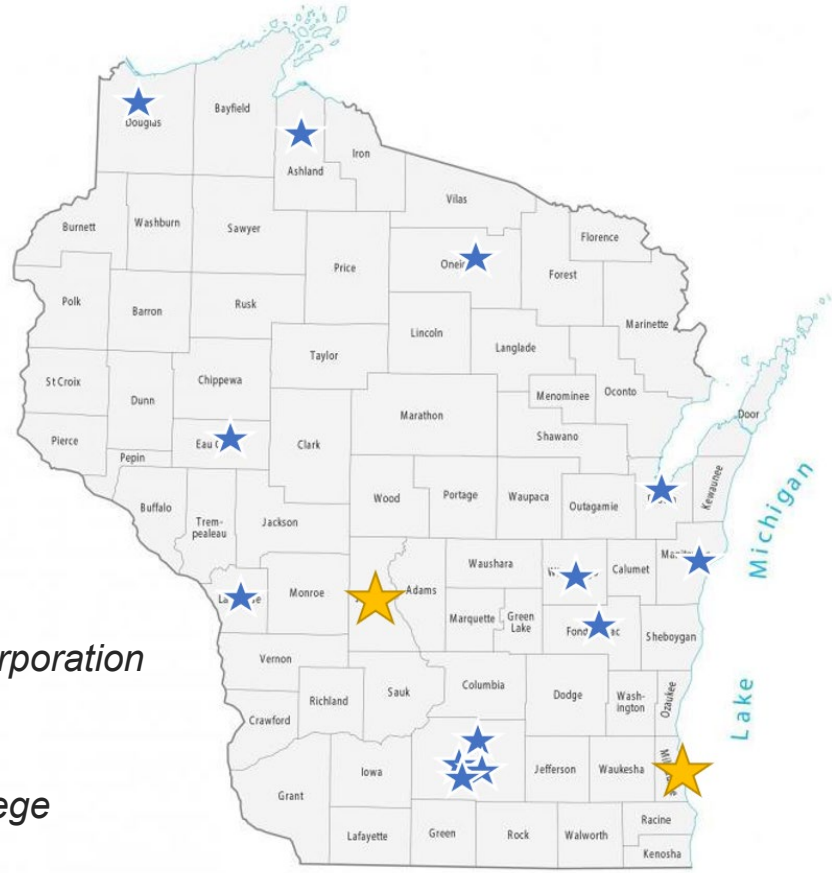
The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

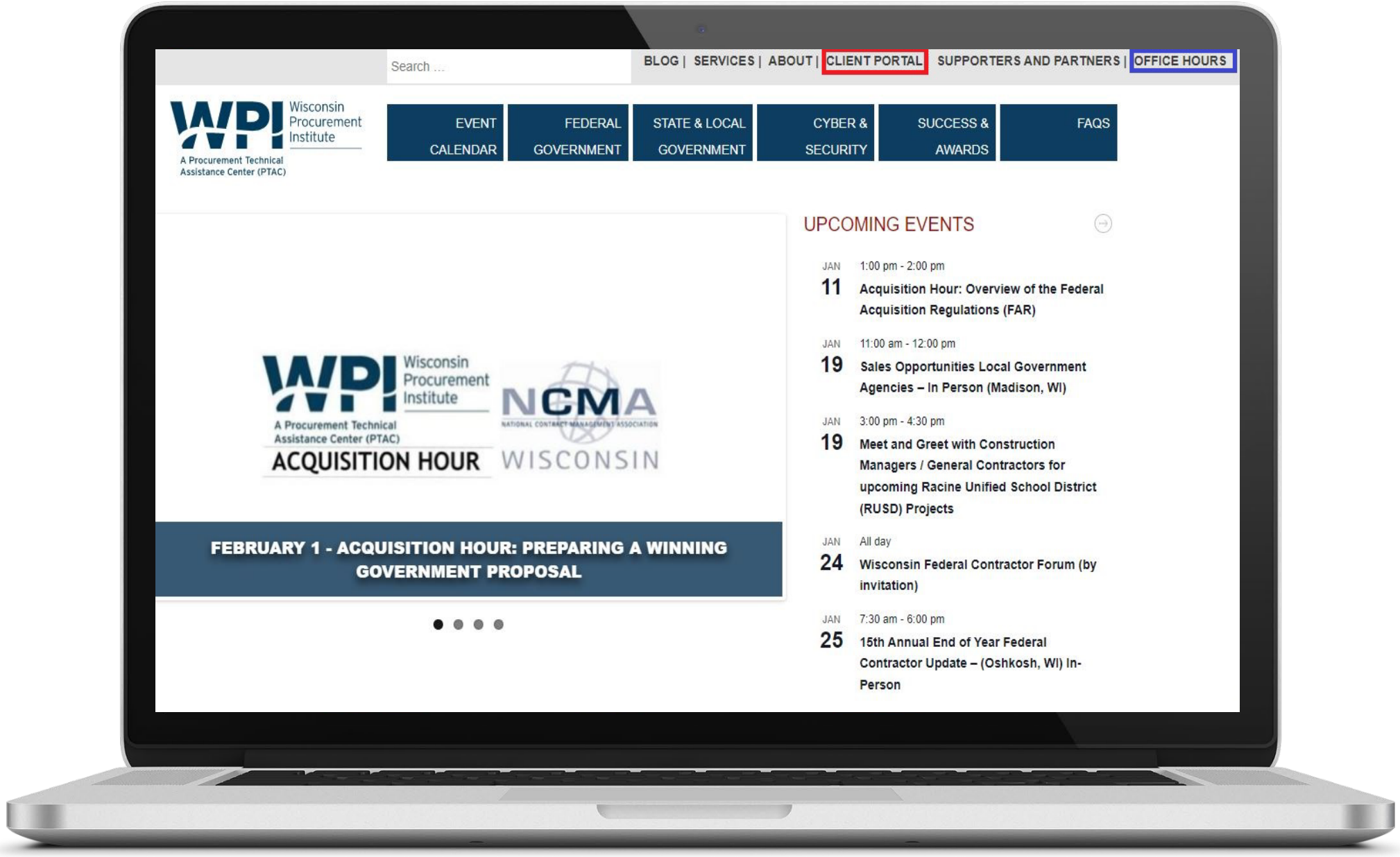
More about WPI

- 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……
- Last year WPI sponsored or participated in over 80 events
- Last year WPI provided technical assistance to over 1300 companies
- The APEX Accelerator is funded in part through a cooperative agreement with the Department of Defense
- WPI is also funded by the Wisconsin Economic Development Corporation (WEDC), contributions and in-kind

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*

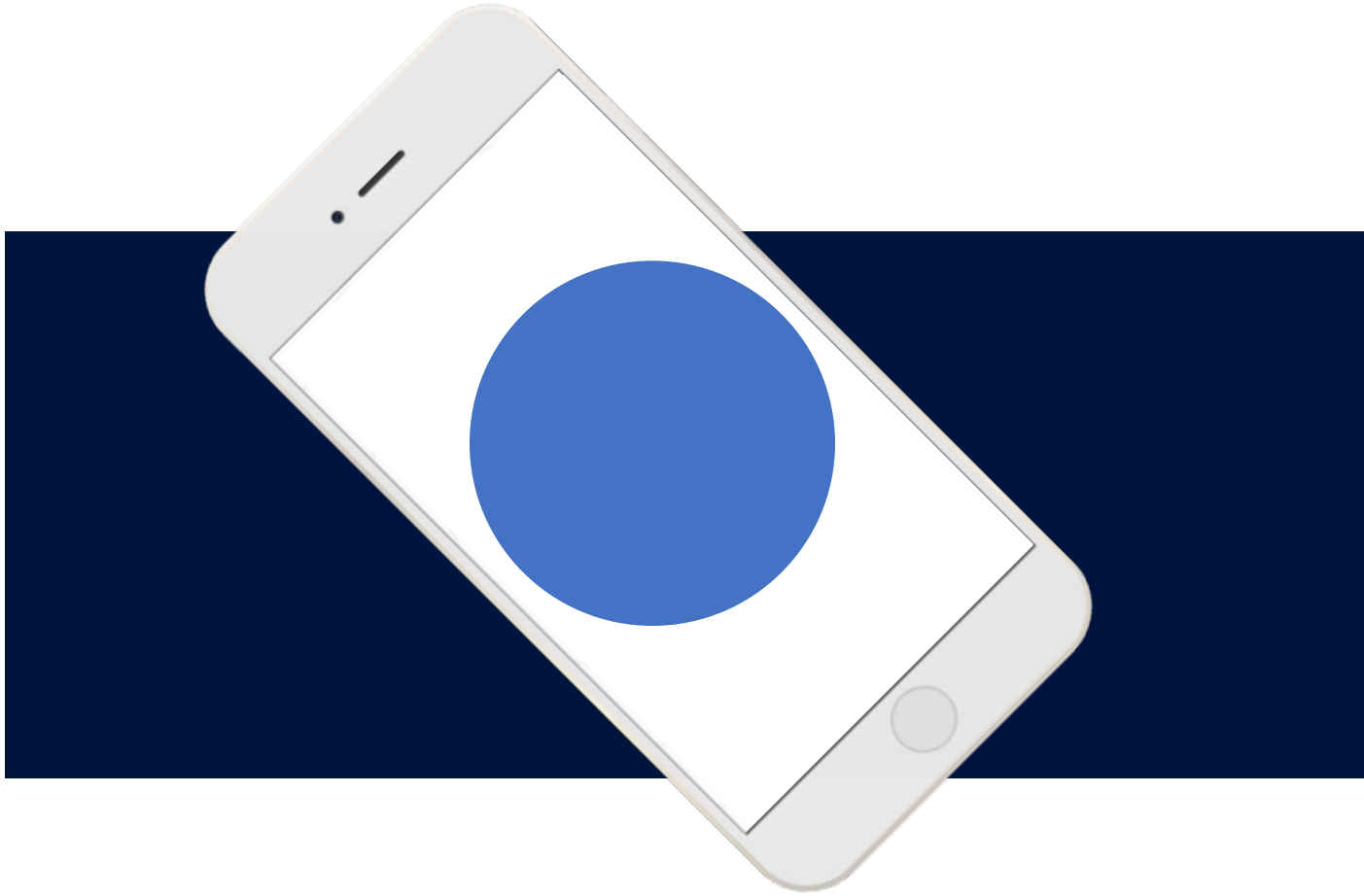



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
WPI Wisconsin Procurement Institute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

Preparing for a Cyber Incident

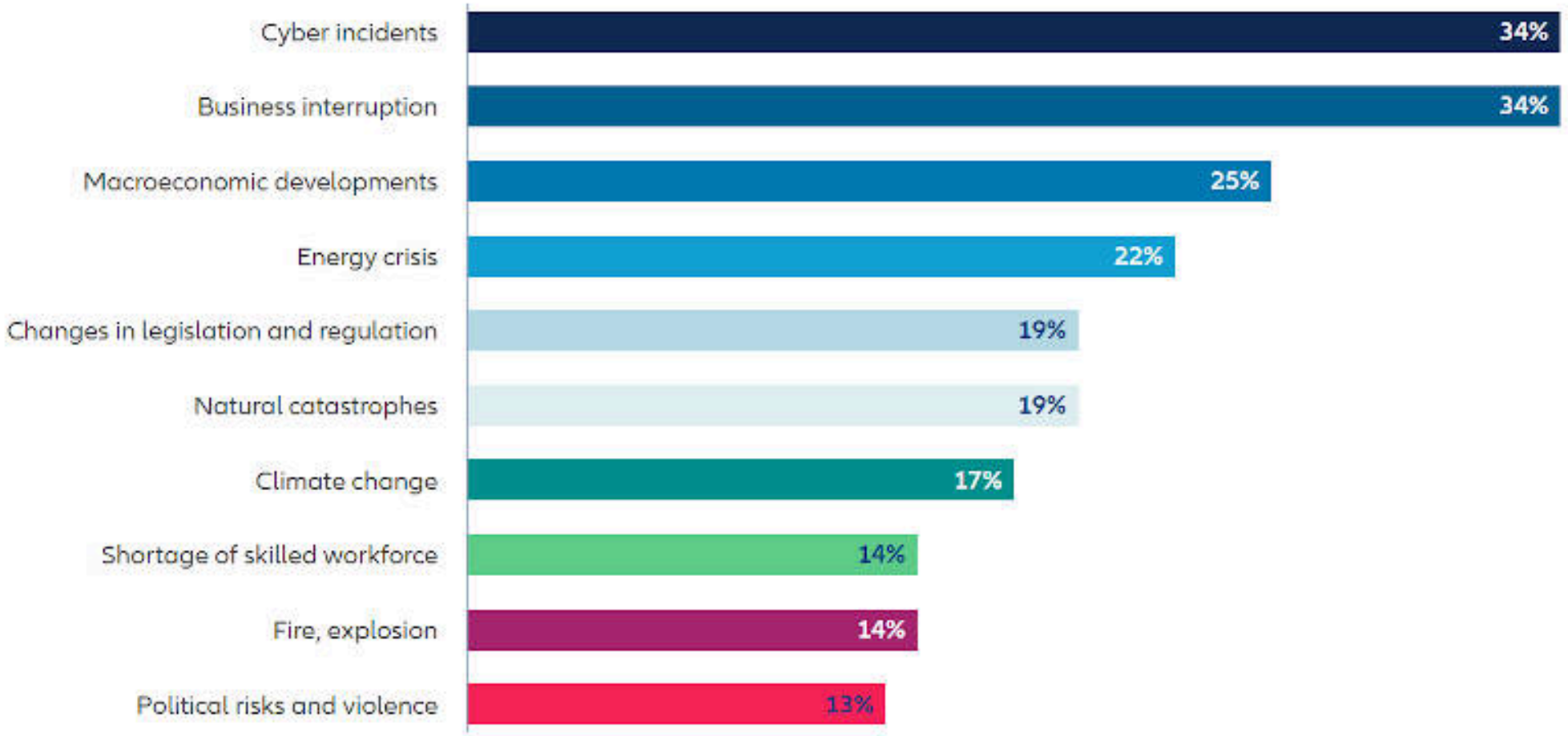
Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – March 10th, 2023

Why prepare?



Source: Allianz Risk Barometer 2023

The numbers represent the percentage of all participants who responded (2,712). The numbers do not add up to 100% because more than one risk could be selected.

DFARS 252.204-7012

NIST
National Institute of Standards and Technology

The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017.

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

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.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61 Revision 2

Computer Security Incident Handling Guide

1. NIST SP 800-61
   NIST Special Publication 800-61 Revision 2 Computer Security Incident Handling Guide
2. CISA
   Department of Homeland Security's Cybersecurity & Infrastructure Security Agency
3. NIST SP 800-171A
   NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information

The Incident Response Plan

NIST SP 800-61

1 PREPARE

2 THE INCIDENT

3 POST-INCIDENT

What is Incident Response?

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.

SCOPE

Scope

Outline the scope of the incident response plan. If contractors, clients or other visitors fall under the plan, note that.

For example:

This incident response plan applies to all employees, contractors, clients and visitors of [Company Name]. This plan does not cover cybersecurity incidents or data breaches. For information about responding to incidents involving information systems and networks of [Company Name], see the Cybersecurity Incident Response Plan.

OR

This incident response plan applies to the information systems and networks of [Company Name] as well as any person or device that gains access to these systems or their data. For more information about responding to incidents involving physical security or workplace safety at [Company Name], see the Workplace Incident Response Plan.

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

Prioritizing Incidents

Incident Prioritization Matrix

Urgency	Impact: High-System Wide Business Unit, Department, Location	Impact: Medium-Multiple Users Number of Users	Impact: Low-Single User Single User
High Can no longer perform primary work functions	**Critical**	**High**	**Moderate**
Medium Work functions impaired, the workaround in place	**High**	**Moderate**	**Low**
Low Inconvenient	**Moderate**	**Low**	**Low**

invgate

BUSINESS CONTINUITY

TRACKING ORDERS/SERVICE REQUESTS

With your infrastructure down – how can you recover information about orders in-process or recently placed?

CONTINUING PRODUCTION

Can you operate and produce despite network services potentially being down? How long can this operate? How will this process transition back to a digital process?

SHIPPING PRODUCT

Without network access how do shipments work?

COMMUNICATIONS

The Incident Response Plan

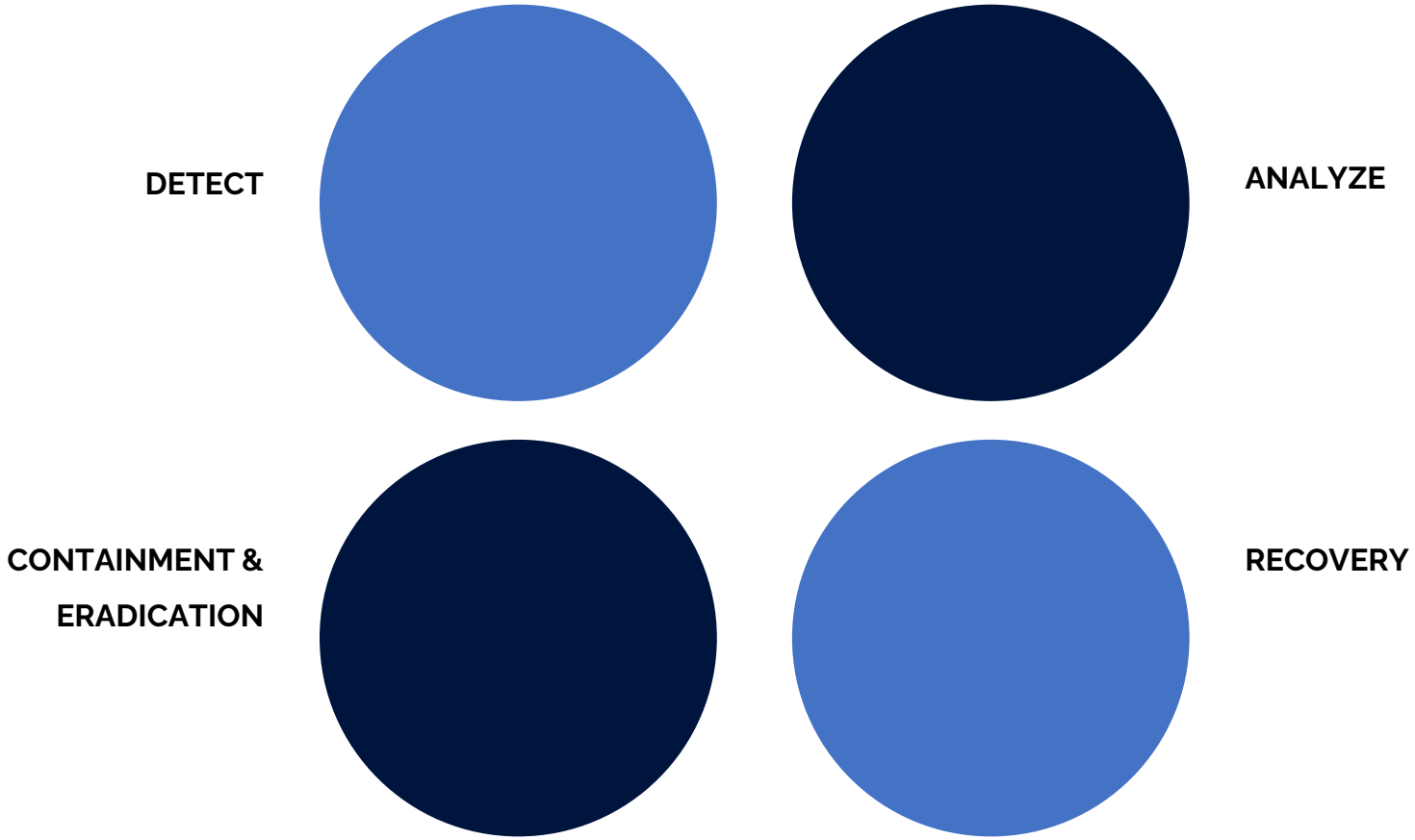
NIST SP 800-61

1 PREPARE

2 THE INCIDENT

3 POST-INCIDENT

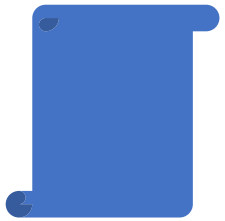
Plan of Action and Milestones



COMMUNICATIONS

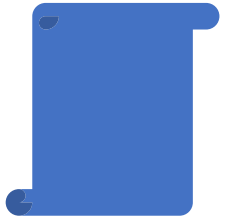
HOW CAN YOU HAVE AN ANOMALY IF YOU DO NOT HAVE CONSISTENCY?

Containing an Incident



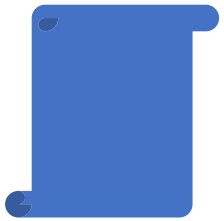
1. Isolate

- ❑ Disconnect From Network
- ❑ Do not Shutdown or Reboot
- ❑ Sandbox (Endpoint Protection)
- ❑ Approval if cannot be isolated



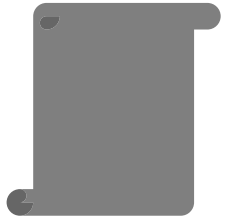
2. Indicators of Compromise

- ❑ Geographic Irregularities
- ❑ Unknown Applications
- ❑ Unusual Activity from Accounts
- ❑ Requests of Additional Permissions
- ❑ Unusual Outbound Traffic
- ❑ Increased Log-In Failures
- ❑ Database Read Volume Increases
- ❑ Unauthorized Changes



3. Copy

- ❑ Copy or Preserve Compromised Systems
- ❑ Capture Executables/Applications
- ❑ Diagram/Log/Journal Incident Details and Events



4. Backups

BACKUPS and BASELINES

What's a Backup?

Data Backup

[da·ta·back·up] **noun**

A copy or archive of your important information on a device.

The act of **backing up your data** is when you:

Create a copy of your important information.

Store it in a secure, separate location.

Recognize the backup as a restoration method for your device.

The Incident Response Plan

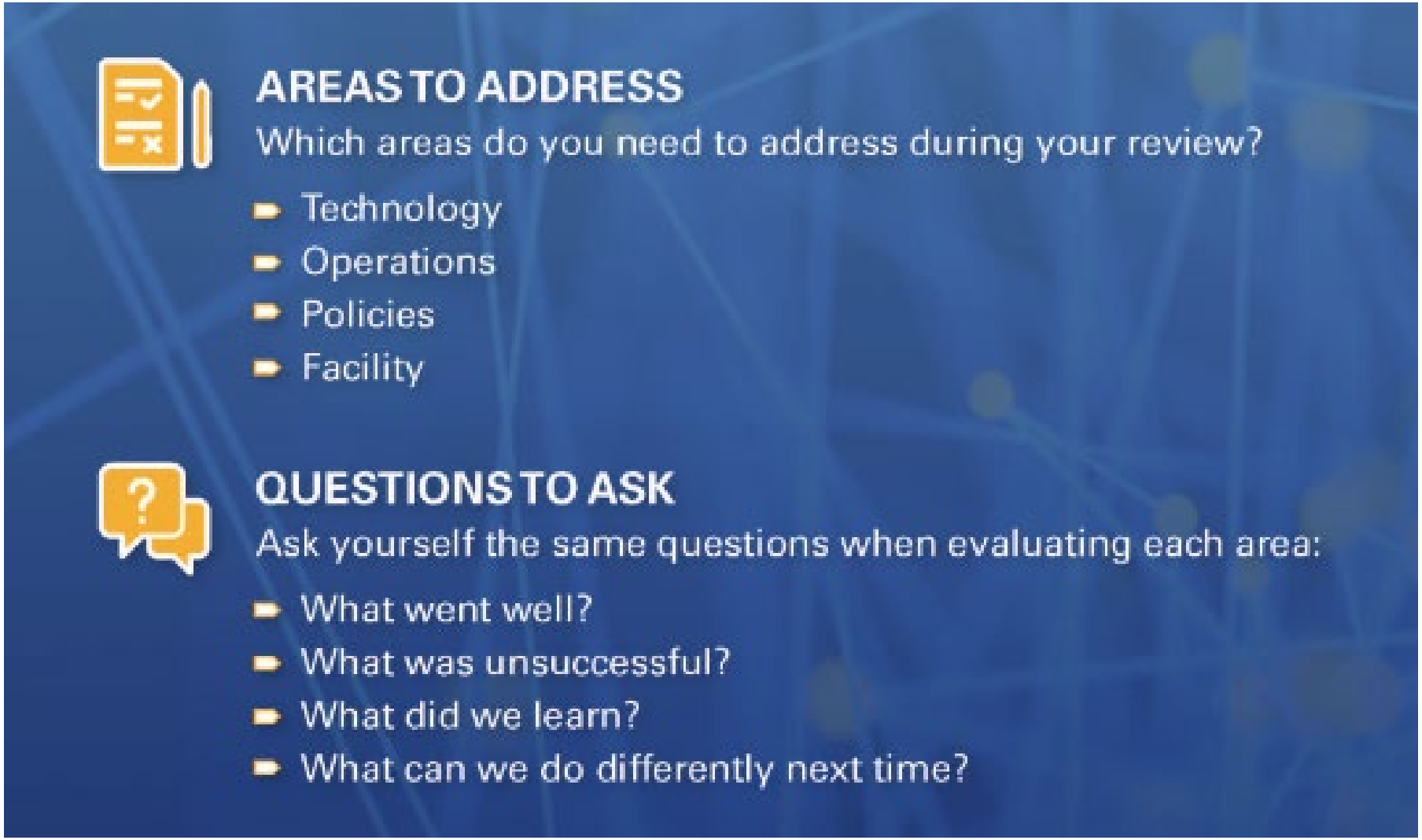
NIST SP 800-61

1 PREPARE

2 THE INCIDENT

3 POST-INCIDENT

Post-Incident Review



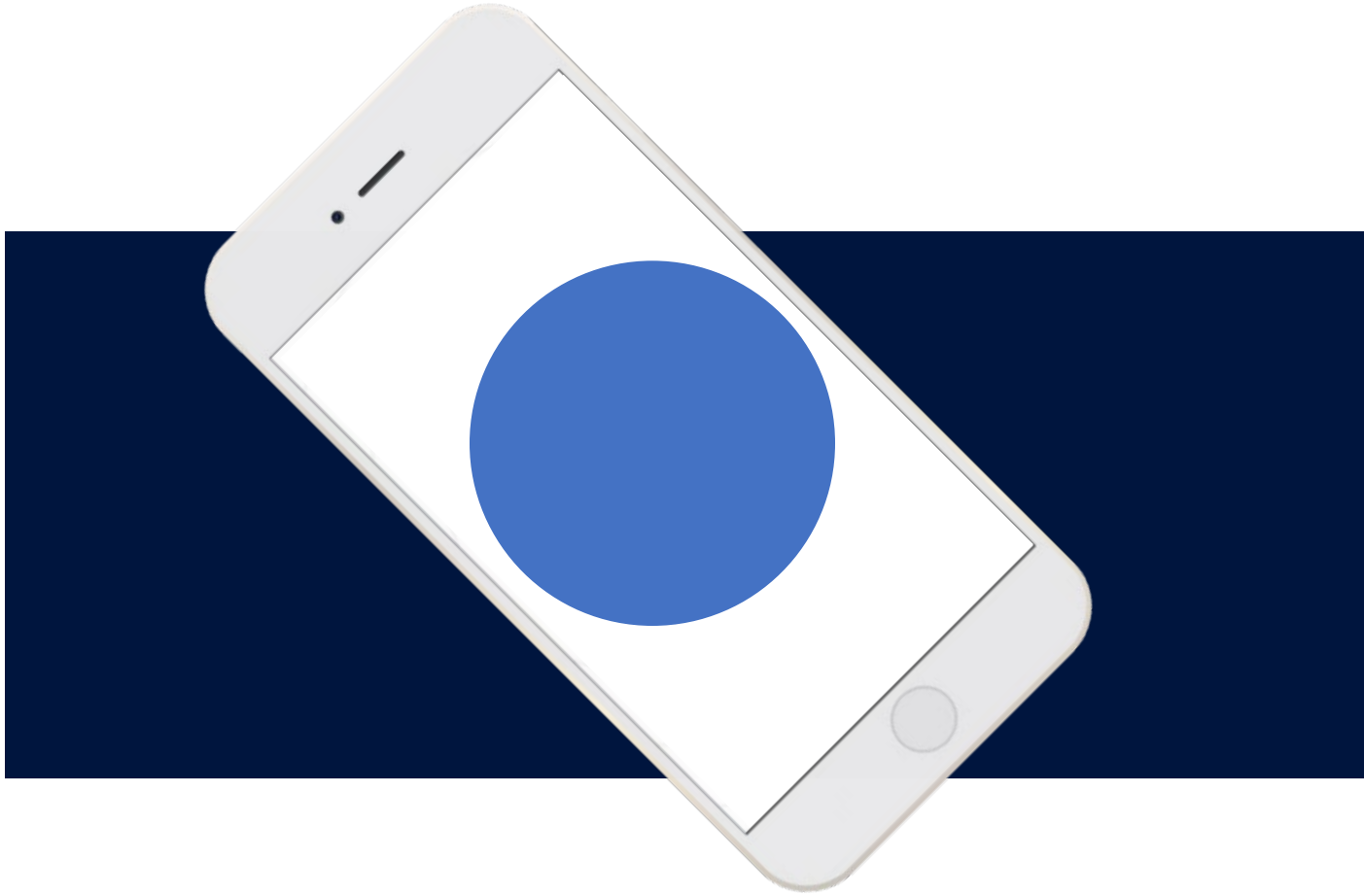
Post-Incident Review

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

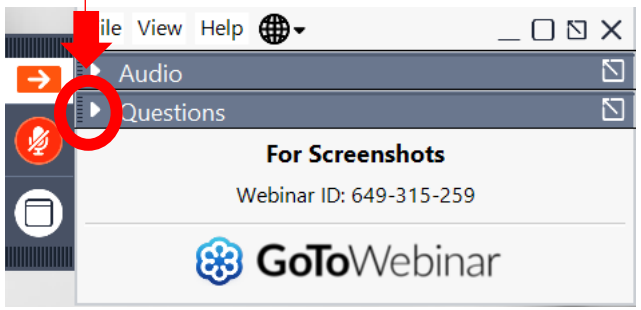
AN APEX ACCELERATOR



QUESTIONS?

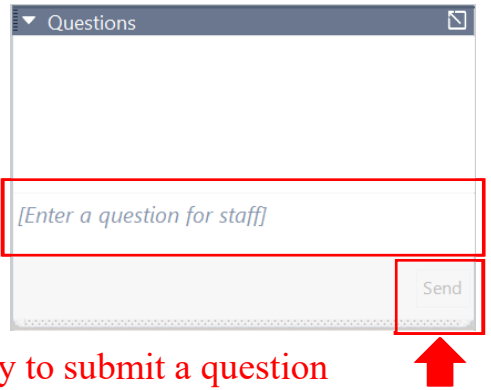
OPENING THE QUESTIONS BOX

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

ACQUISITION HOUR LIVE WEBINAR SERIES

- April 5
  Overview of Contractor Performance Assessment Reporting System (CPARS)
- April 19
  No-Cost Federal Market Research Tools: SAM.gov, DSBS, and USA Spending
- May 9
  The Procurement Integrated Enterprise Environment (PIEE) – Wide Area Workflow (WAWF)
- June 6
  Government Furnished Property

…More information and registrations at wispro.org/events

CYBER FRIDAY LIVE WEBINAR SERIES

- March 10
  Preparing for a Cyber Incident
- March 24
  Protecting the Data
- April 14
  The Forensic Record
- April 28
  Culture of Security

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

DOD Supply Chain: Cyber Workshop

Wisconsin manufacturers are facing a significant challenge in meeting cyber and security compliance requirements that are being included in their Defense, Federal and commercial contracts and subcontracts.

Join us at one of the following in person sessions to learn from a veteran of the IT Industry as he provides insights and guidance on what manufacturers can do to improve their security position in a rapidly shifting digital landscape while positioning themselves to meet both existing and upcoming supply chain requirement (such as NIST SP 800-171, CMMC, ITAR).

All session are scheduled for 10 am - Noon

March 9
Envision Greater Fond Du Lac
23 S Main St Ste 101
Fond du Lac, WI 54935

March 15
Progress Lakeshore
202 N 8th St Ste 101
Manitowoc, WI 54220

March 21
Greater Oshkosh EDC
100 N Main St Ste 104
Oshkosh, WI 54901

wispro.org/events

March 10, 2023

SURVEY

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR

March 10, 2023

APEX ACCELERATORS

CONTINUING PROFESSIONAL EDUCATION

This webinar is eligible for 1 CPE credit.
For a certificate of this credit please contact:

Caroline Boettcher
carolineb@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