Wisconsin Procurement Institute

AN APEX ACCELERATOR

APEX ACCELERATORS

CYBER FRIDAY: PREPARING FOR SELF-ASSESSMENT

February 10, 2023 @ 11:00 am - Noon

Presented by Matt Frost, WPI

Webinar Etiquette

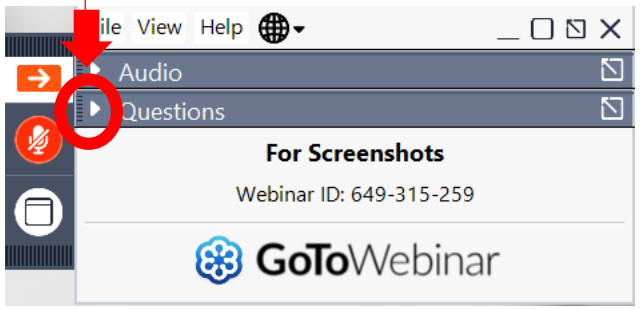
PLEASE

- 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!

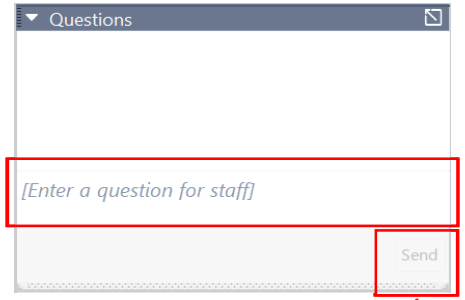
OPENING THE QUESTIONS BOX

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

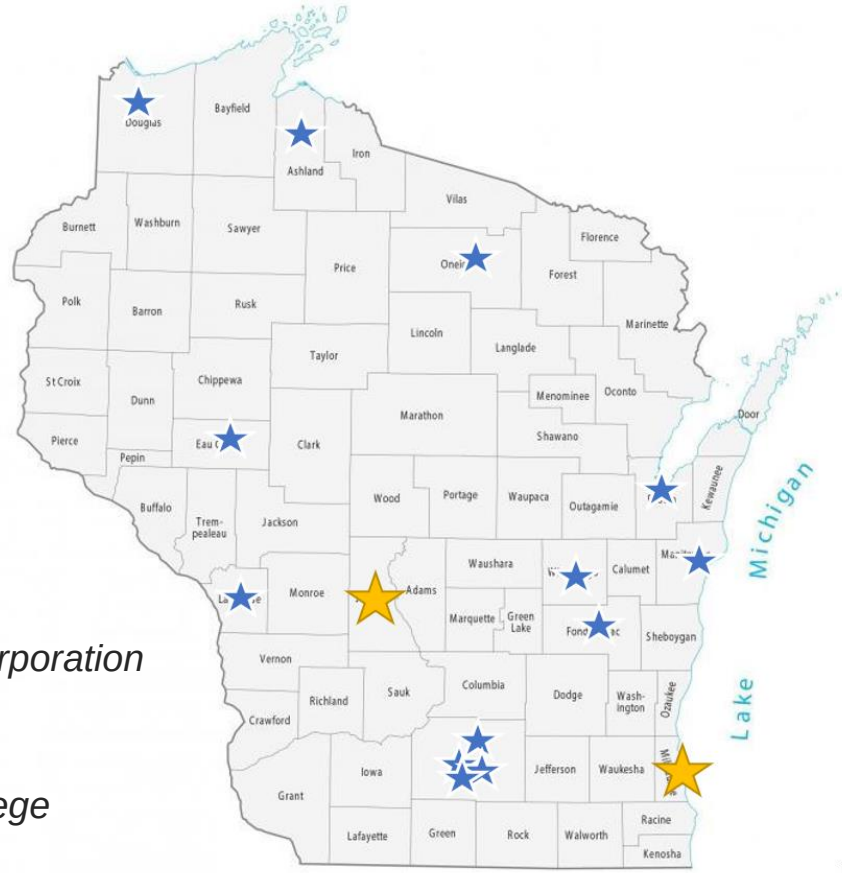
WPI is Wisconsin's APEX ACCELERATOR

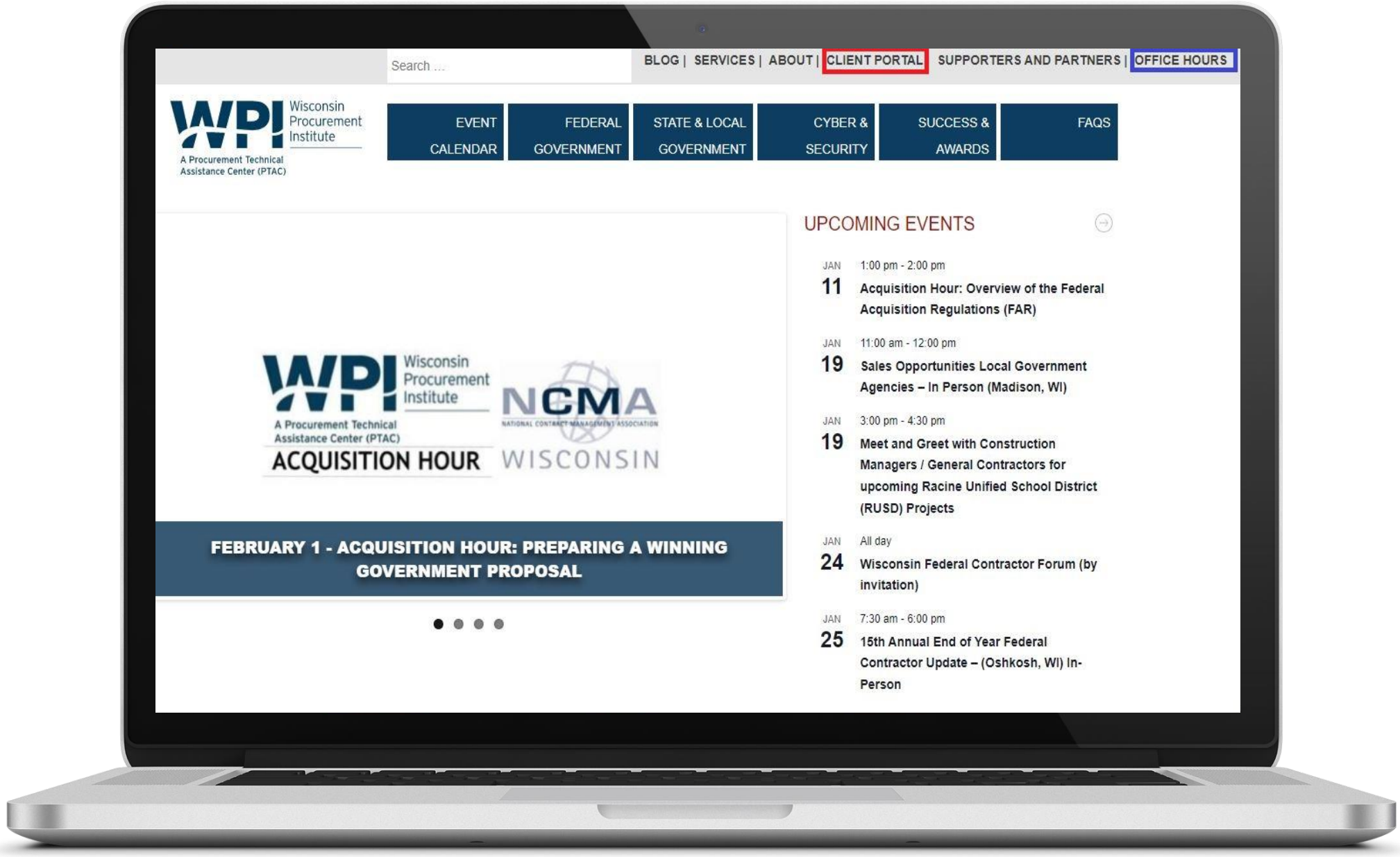
The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides 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 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*

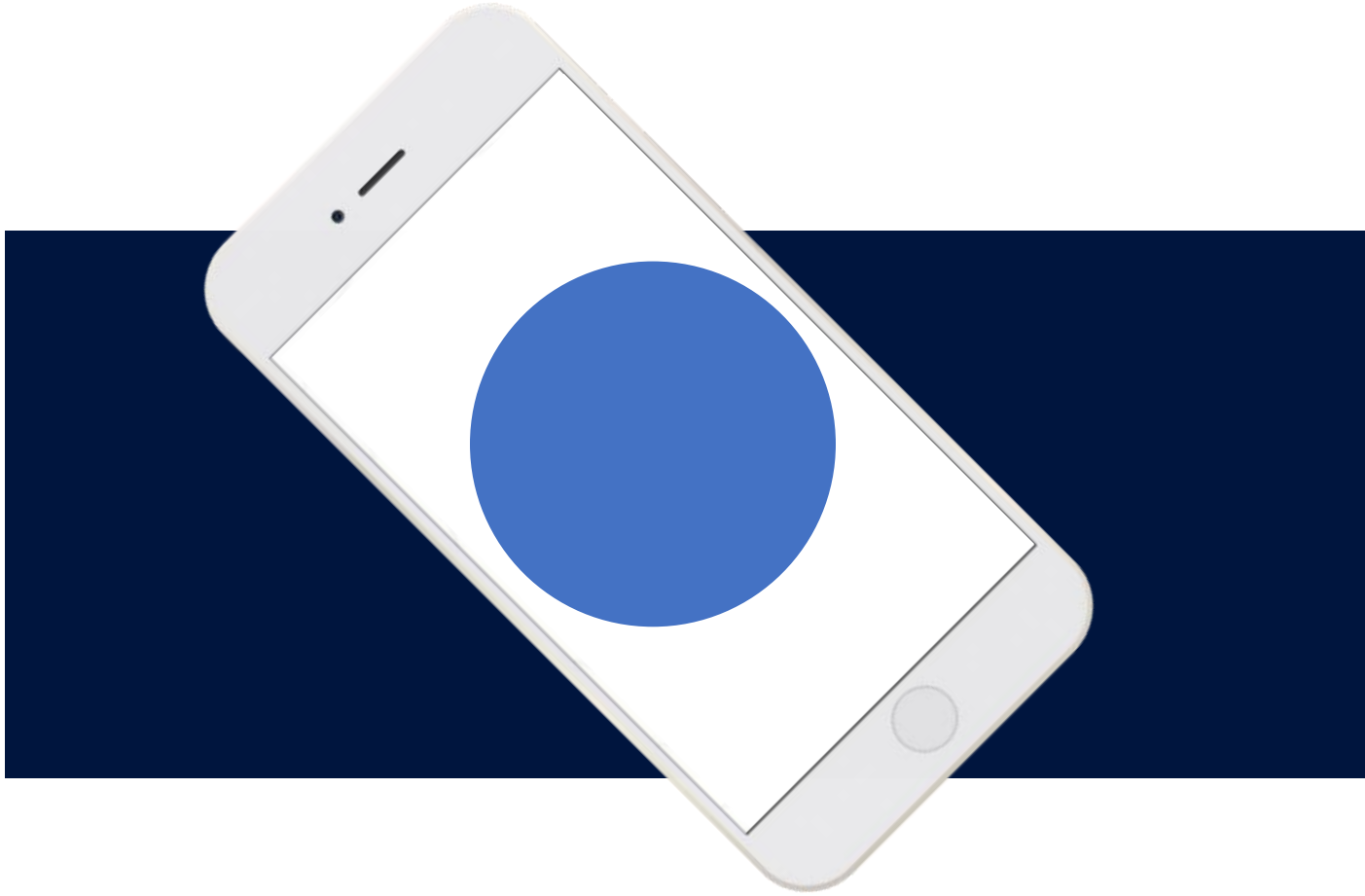



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
Wisconsin Procurement Institute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

Wisconsin Procurement Institute

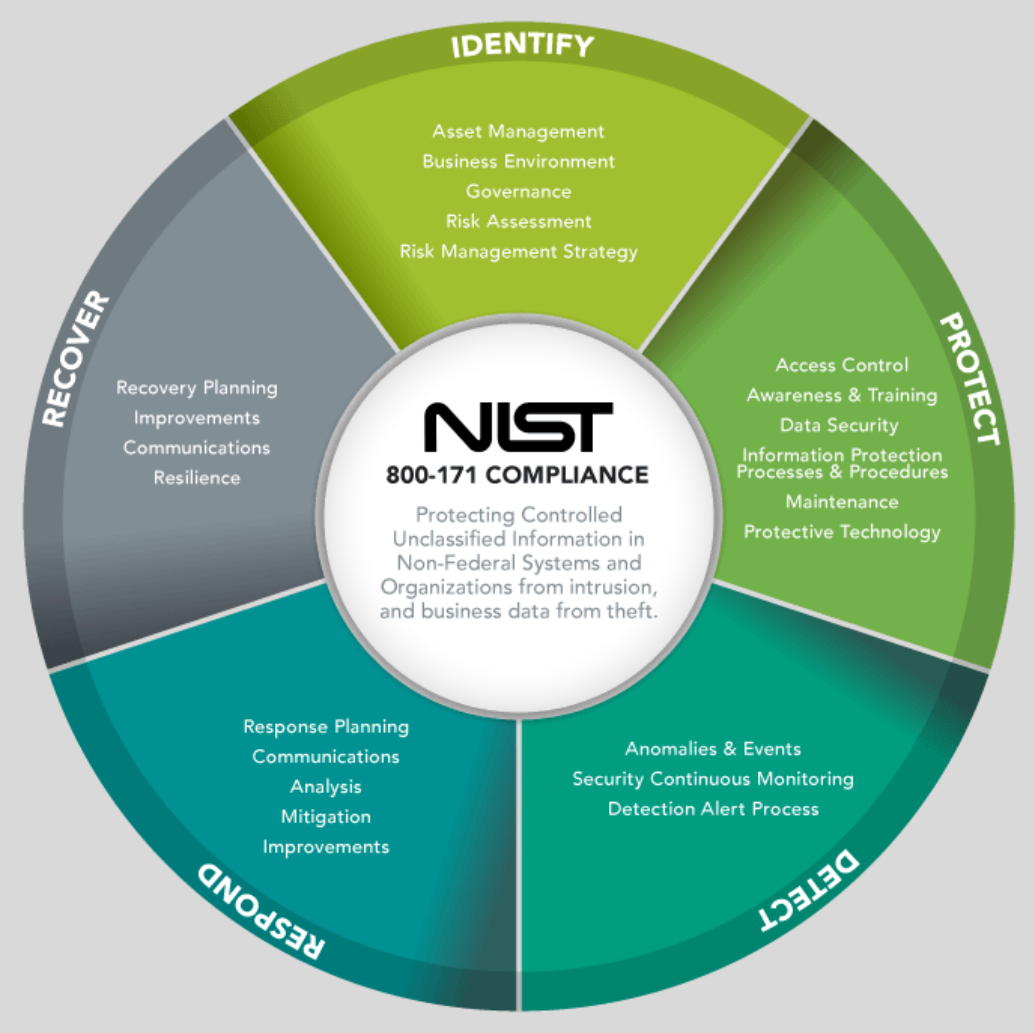
AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – February 10th, 2023

DFARS 252.204-7019

NIST SP 800-171 DOD Assessment Requirements
(Provision)



NIST Basic Assessment and Score

- ❑ Conduct a NIST SP 800-171 Basic Assessment
- ❑ Post Summary Level Scores in the Supplier Performance Risk System (SPRS)
- ❑ Summary Level Scores cannot be older than 3 years

Why a Self-Assessment?

DFARS 252.204-7019

DFARS 252.204-7020

- Effects all contracts awarded on and after 30 NOV 2020.
- No existing minimum score requirements.
- Prime Contractor cannot access your score in SPRS – they must request from vendor directly.

DFARS 252.204-7012

Safeguarding Covered Defense Information and Cyber Incident Reporting

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.

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.

The Self-Assessment Process

NIST SP 800-171

1 — **PREPARE**

2 — **ASSESS**

3 — **REPORT**

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

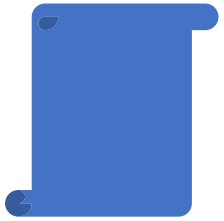
NIST Special Publication 800-171A Assessing Security Requirements for Controlled Unclassified Information

3

DoD Memo

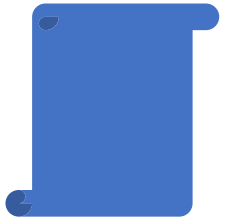
DoD Memo
DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements

Internal Documentation



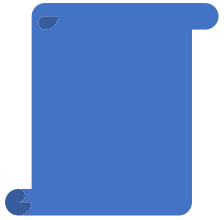
System Security Plan

A formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.



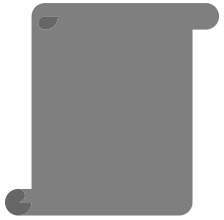
Incident Response

The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).



Security Training

Training documentation provided to employees to improve their ability to respond to cyber attacks and protect confidential information.



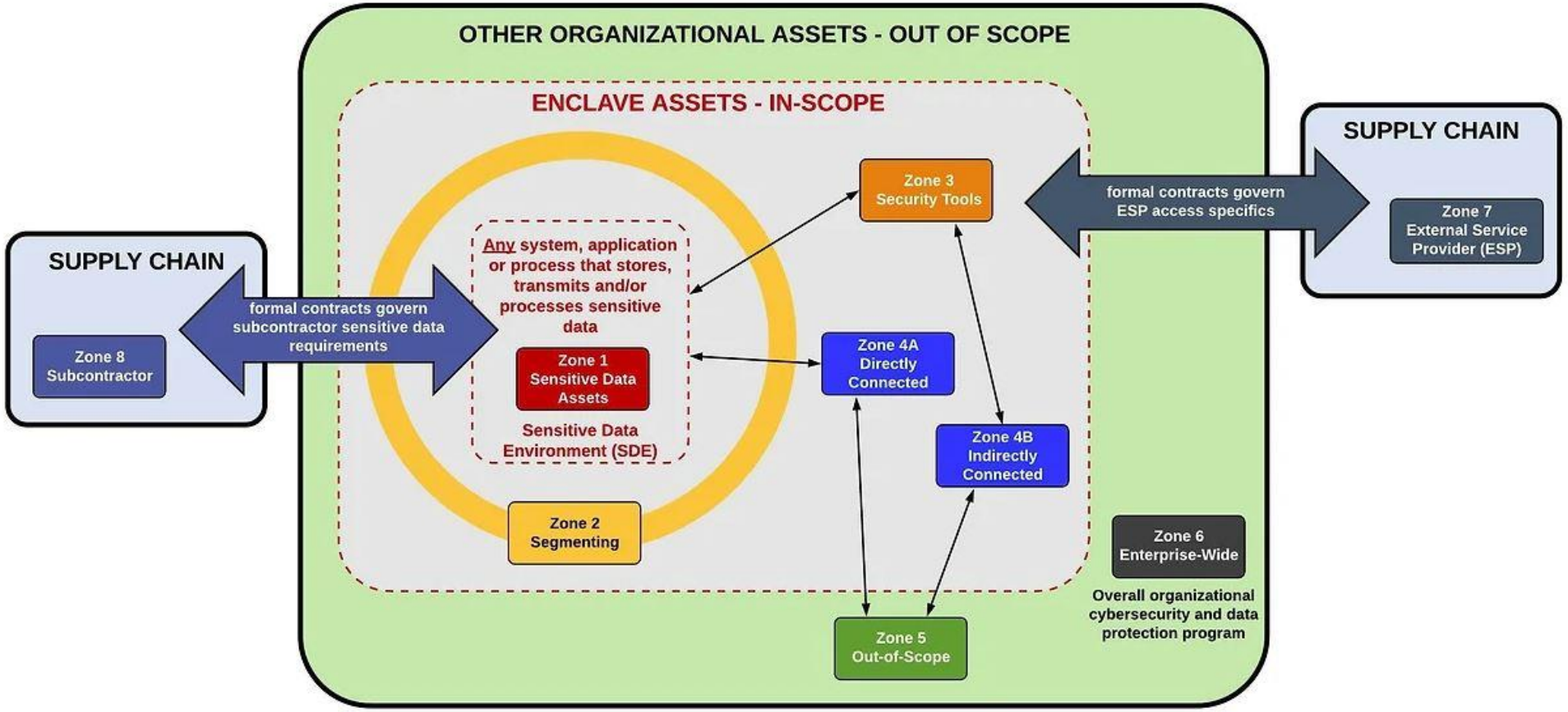
Prior Assessments

Previously conducted assessments.

Additional Internal Documents

- Business Continuity Plans
- Disaster Recovery Plans
- Plan of Action and Milestones
- Acceptable Use Plan
- Business Process Flow
- Network Diagram

SCOPING THE ASSESSMENT



INFORMATION

- CUI (Drawings, Parts Lists)
- FCI (Contracts, RFQs)
- EAR/ITAR

SECURITY ASSETS

- Digital Hardware
- Software
- Cloud Services

PRINTED MATERIAL

- Job Travelers
- Diagrams & Drawings
- Work Instructions / TO's

PERSONNEL

- U.S Persons
- Principle of Least Privilege

The Self-Assessment Process

NIST SP 800-171

1 — **PREPARE**

2 — **ASSESS**

3 — **REPORT**

Who Performs the Assessment?

System Owner

- ❑ Ensures Cooperation
- ❑ Identifying Key Individuals
- ❑ Identifying Delegated Responsibilities
- ❑ Identifying Business Priorities

IT Manager

- ❑ Technical Expertise
- ❑ Defines Implementation
- ❑ Identifies Technical Shortfalls
- ❑ Explains Cyber Risks

Security Officer

- ❑ Determines whether Control is adequately met
- ❑ Defines Control Requirements
- ❑ Identifies Procedural Shortfalls

Operations Manager

- ❑ Defines work flow.
- ❑ Highlights use of applications.
- ❑ Explains operational needs and challenges

Assessment Process

ASSESSMENT OBJECTIVES

Includes a determination statement related to the CUI security requirement that is the subject of the assessment.

Ex. 3.1.3 Control the flow of CUI in accordance with approved authorizations

ASSESSMENT METHODS

Define the nature and the extent of the assessor's actions. They include **examine**, **interview**, and **test**.

Ex. 3.1.3 Examine architectural solutions to control flow of system data.

ASSESSMENT OBJECTS

Identify specific items being assessed and can include specifications, mechanisms, activities, and individuals.

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

Assess each of the NIST SP 800-171 controls using the NIST SP 800-171A to ensure all audit points are covered.

3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.3[a] *information flow control policies are defined.*
	3.1.3[b] *methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c] *designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d] *authorizations for controlling the flow of CUI are defined.*
	3.1.3[e] *approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].

3.1.3 Control the flow of CUI in accordance with approved authorizations.

Do you have architectural solutions to control the flow of system data?

Yes No Partially Does Not Apply Alternative Approach

Do you document information flow control enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?

Yes No Partially Does Not Apply Alternative Approach

Additional Information

The solutions may include firewalls, proxies, encryption, and other security technologies. Information flow control regulates where information can travel within an information system and between information systems (as opposed to who is allowed to access the information) without explicit regard to subsequent accesses to that information.

Examples of flow control restrictions include:

- keeping export-controlled information from being transmitted in the clear to the internet,
- blocking outside traffic that claims to be from within the organization,
- restricting web requests to the internet that are not from the internal web proxy server, and
- limiting information transfers between organizations based on data structures and content.

Where to Look:

- access control policy
- information flow control policies
- procedures addressing information flow enforcement
- information system design documentation
- information system configuration settings and associated documentation
- information system baseline configuration
- list of information flow authorizations information system audit records
- other relevant documents or records

Who to Talk to:

- system/network administrators
- employees with information security responsibilities
- system developers

Perform Test On:

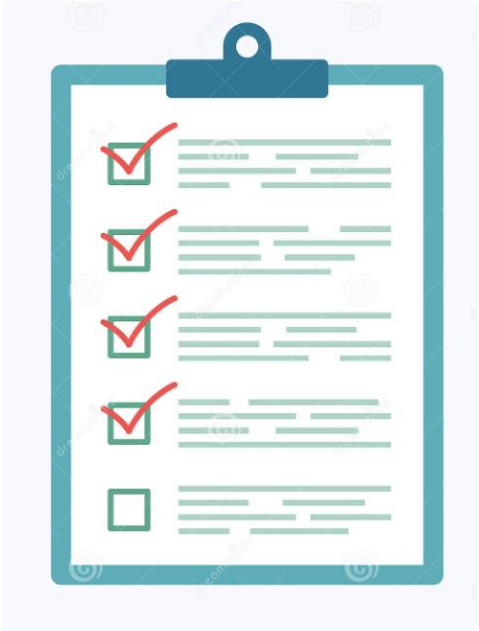
- automated mechanisms implementing information flow enforcement policy

The Self-Assessment Process

NIST SP 800-171

1 — **PREPARE**

2 — **ASSESS**



3 — **REPORT**

Clearly document the requirement, objectives, and methods of observation.

Ensure all Objectives within the Control are met to the fullest of your ability.

DOCUMENT FINDINGS

3.1.1 (AC.L1) Control the flow of CUI in accordance with approved authorizations.

- 3.1.3[a] information flow control policies are defined.
  ☒
- 3.1.3[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.
  ☐
- 3.1.3[c] designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.
  ☒
- 3.1.3[d] authorizations for controlling the flow of CUI are defined.
  ☐
- 3.1.3[e] system access is limited to processes acting on behalf of authorized users.
  ☒
- 3.1.3[f] approved authorizations for controlling the flow of CUI are enforced.
  ☒

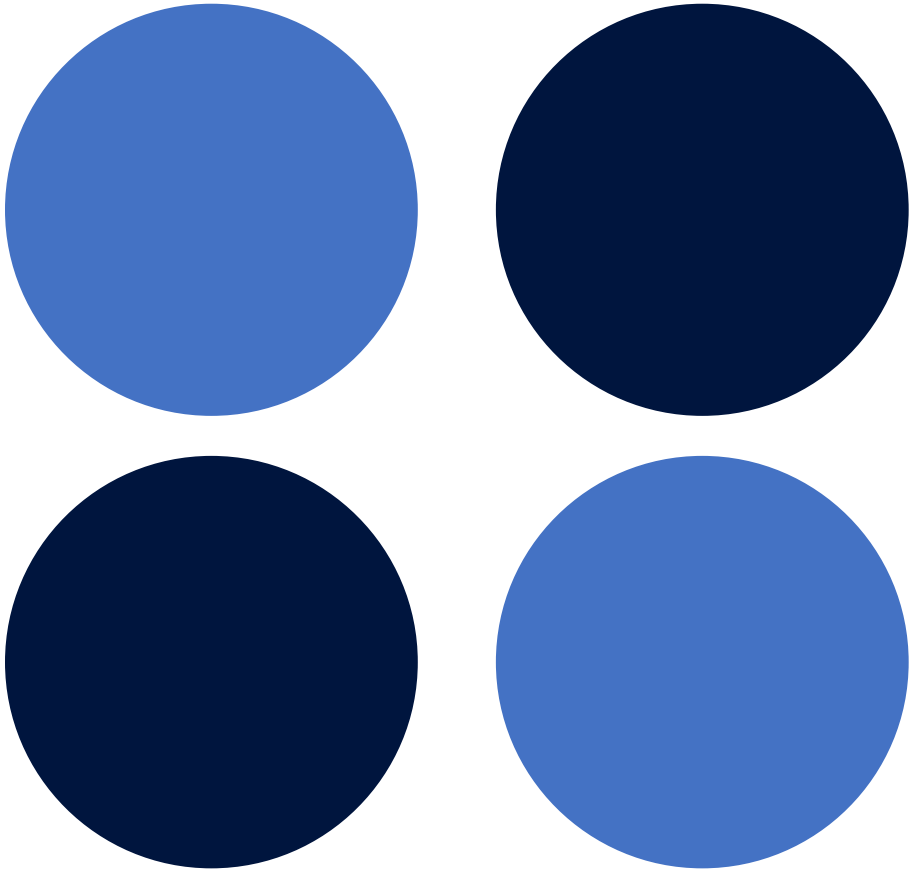
☐Implemented **☒Planned To Be Implemented** **☐Not Applicable**

Notes:

A. No Business Process Flow defined or observed.
B. CUI flow is controlled through policy. Observed policy in SSP.
C. Not Observably Defined.
D. Authorizations require identified and permitted user identifiers unique to the system. Observed test of log-in system to verify access is controlled and controls are functioning according to policy defined in SSP.
E. Processes acting on behalf of users, in necessary job functions, are permitted access to the system. All others are denied by default. Examined Active Directory Users & Computers to verify controls are in place.
F. Accessing CUI, or operating outside of the defined Business Process Flow for CUI, is strictly prohibited on the system. Observed in SSP.

NIST SP 800-171 Summary Score

NIST SP 800-171 can assign 5, 3, or 1 points per control.



NIST Summary Score can range from a -203 to 110.

There is no partial credit for a control. Either all objectives are met or **NO** points are awarded.

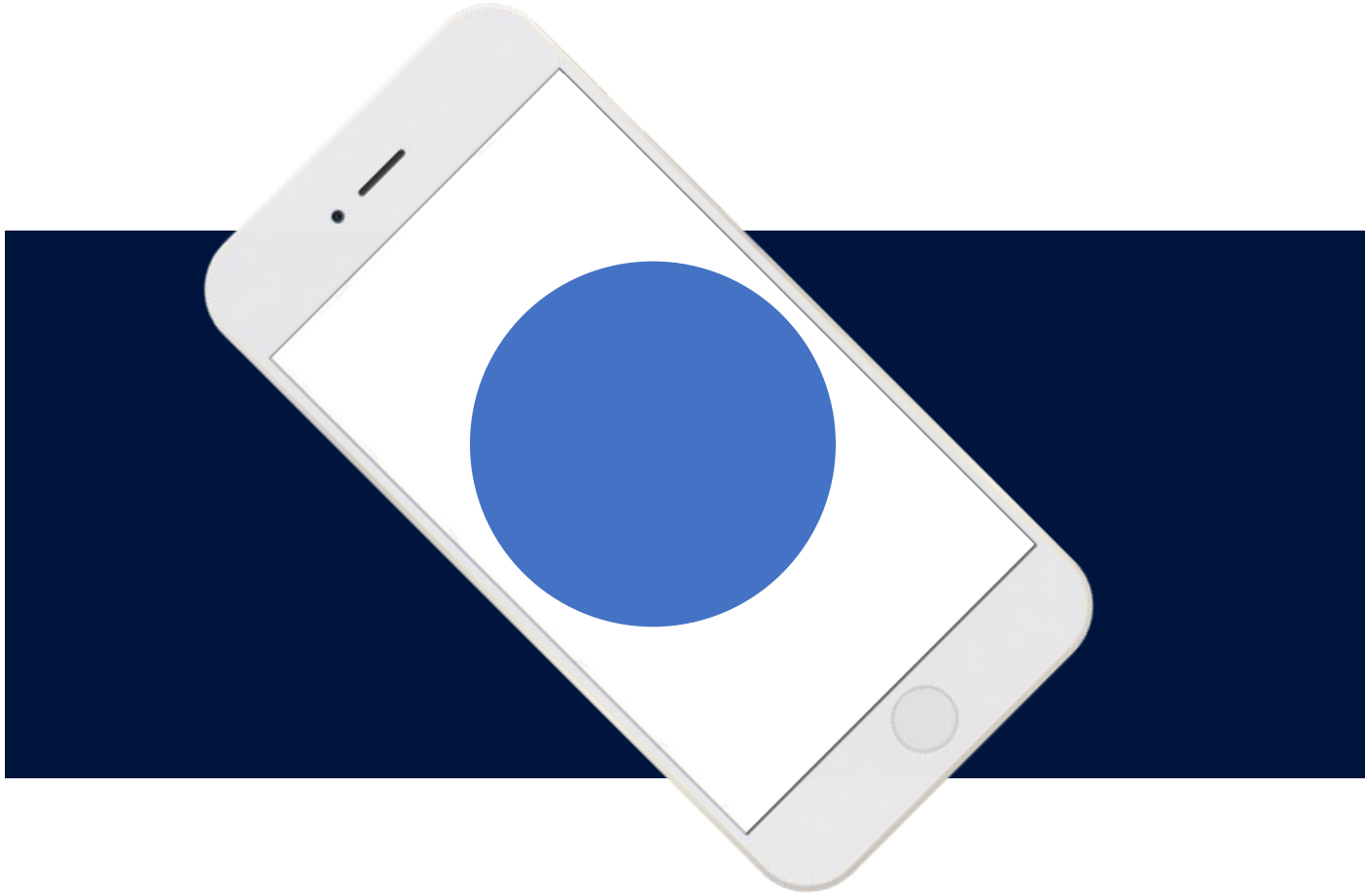
NIST Summary Score must be submitted in SPRS. Cannot be viewed by non-government entities.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

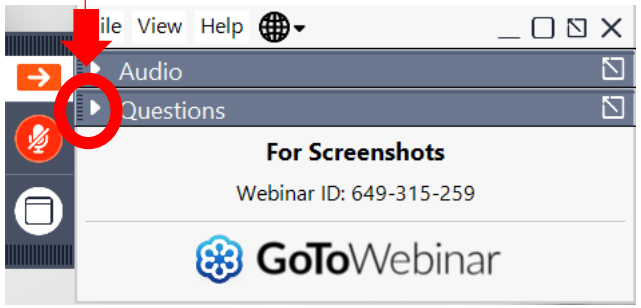
AN APEX ACCELERATOR



QUESTIONS?

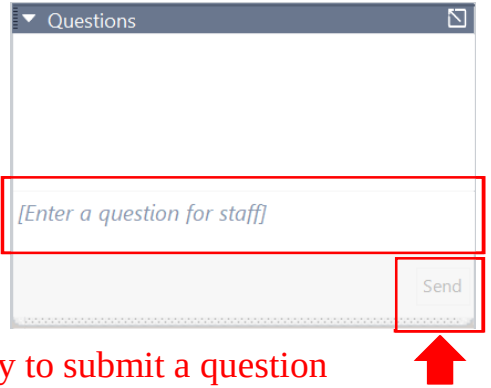
OPENING THE QUESTIONS BOX

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

- March 1
  Service Contracts with Federal Agencies
- March 8
  ESRS Individual Subcontractor Reporting (ISR) Basics
- 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

- February 24
  System Security Plan and Plan of Action and Milestones Construction
- 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

10th Annual WPI and NCMA WI Chapter

FAR Evening Webinar and Study Group Session

Tuesdays, 6:00 – 7:30 pm

February 7 – March 28, 2023

This will be the 10th year that the Wisconsin Procurement Institute (WPI) and the National Contract Management Association (NCMA) Wisconsin Chapter will be hosting and presenting this series.
These sessions are designed specifically for current Federal contractors.
In addition, these sessions will help you prepare for the NCMA CFCM certification exam.
Speaker: Daryl G. Zahn, CFCM, Senior Manager, Contracts and Compliance, Leonardo DRS
This webinar is eligible for 1.5 CPE credits.

Registration now open at
www.wispro.org/events

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

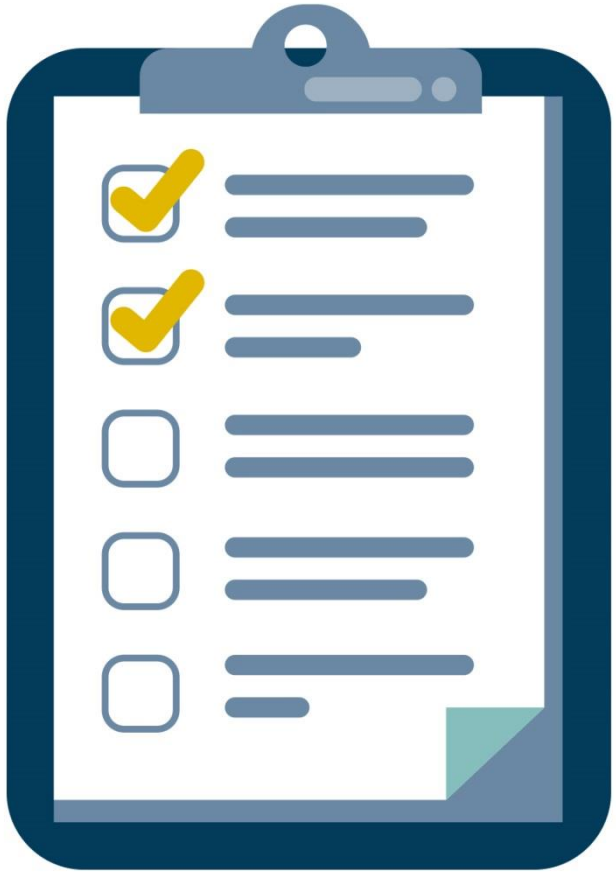
March 15
Progress Lakeshore
202 N 8th St Ste 101
Manitowoc, WI 54220

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

wispro.org/events

February 10, 2023

SURVEY



Wisconsin Procurement Institute
AN APEX ACCELERATOR

February 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