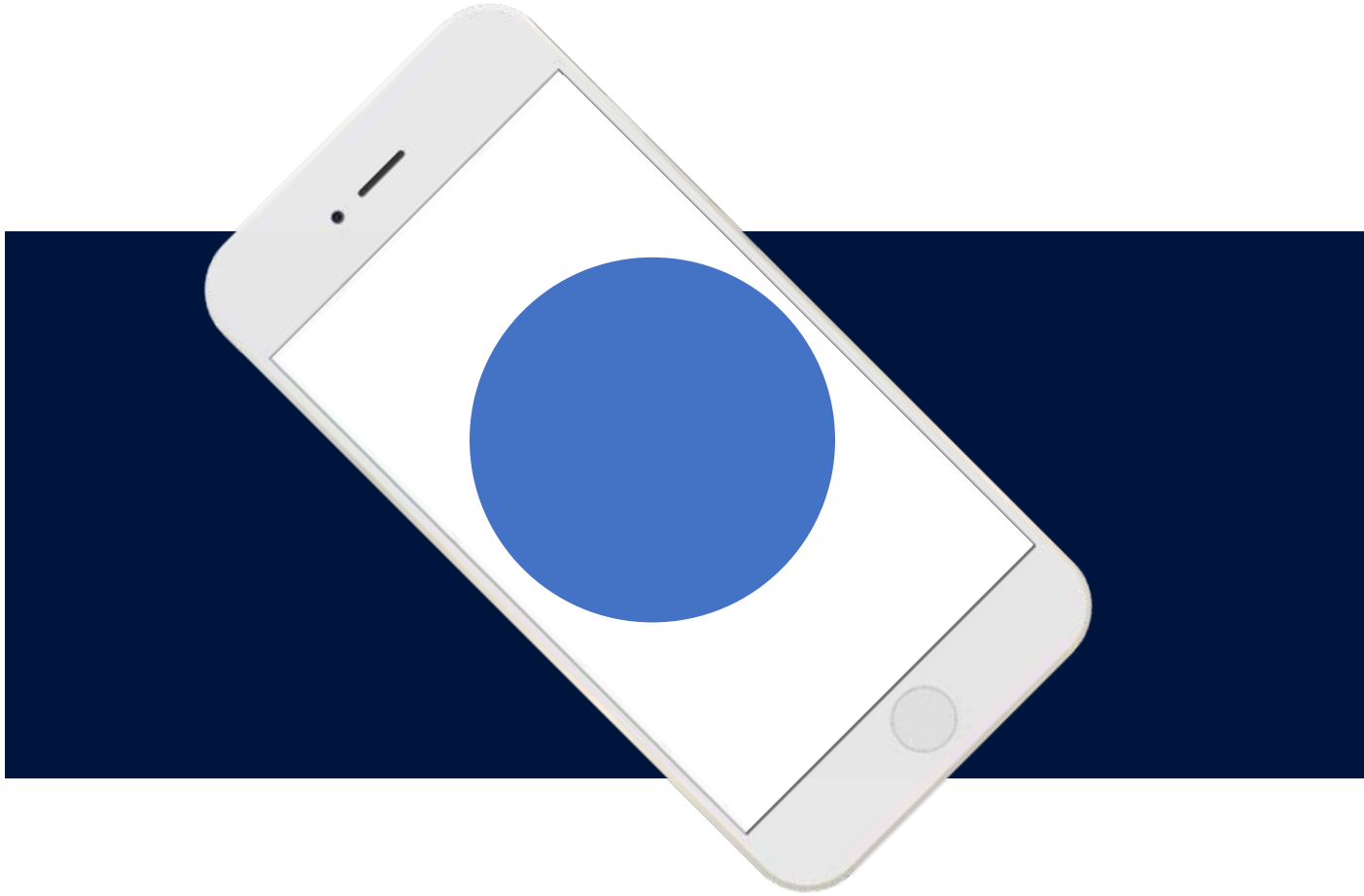
Introduction to NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – November 9th, 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.

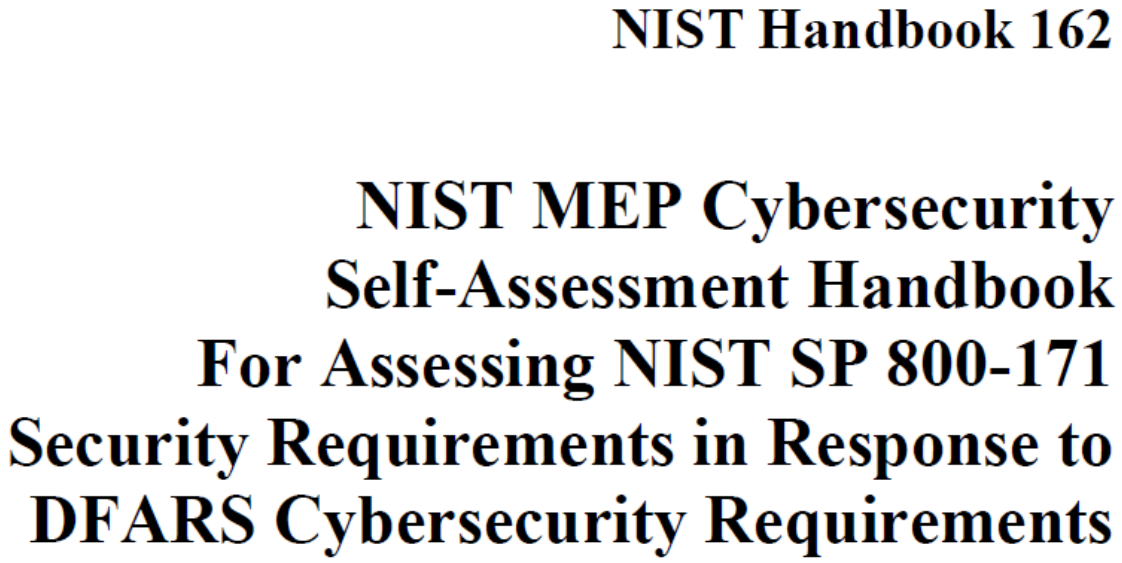
DFARS 252.204-7021

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

System and Communications Protection

SYSTEM

q Enterprise or Enclave

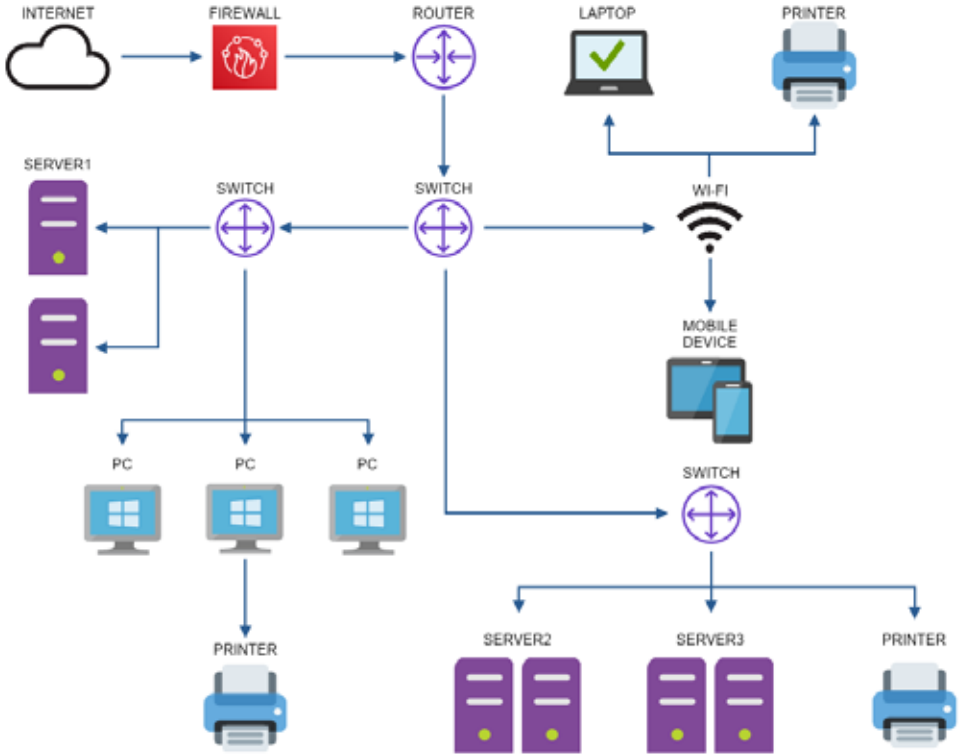
q Collective Environment

q Design, Deployment,

Documentation

IT Heavy Control family

with specific requirements.



COMMUNICATION

q Data In Transit

q Cryptography and Control

q Monitor and Manage

16 Controls with substantial

audit objectives. Artifact

collection key.

3.13.1 **Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.**

DISCUSSION

Communications can be monitored, controlled, and protected at boundary components and by restricting or prohibiting interfaces in organizational systems. Boundary components include gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a system security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Restricting or prohibiting interfaces in organizational systems includes restricting external web communications traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses.

Organizations consider the shared nature of commercial telecommunications services in the implementation of security requirements associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions.

[SP 800-41] provides guidance on firewalls and firewall policy. [SP 800-125B] provides guidance on security for virtualization technologies.

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR
APEX ACCELERATORS

3.13 Basics

Diagram

Policy

Log Review

Control Validation

System and Information Integrity

SYSTEM

q Architecture and Data

q Collective Environment

q Implementation and

Monitoring

Blended family of IT and

Process requirements.

INTEGRITY

q Encrypt

q Scan / Validate

q Response

Show proactive protection

actions as well as

coordinated responses.

3.14.1 **Identify, report, and correct system flaws in a timely manner.**

DISCUSSION

Organizations identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws and report this information to designated personnel with information security responsibilities. Security-relevant updates include patches, service packs, hot fixes, and anti-virus signatures. Organizations address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations can take advantage of available resources such as the Common Weakness Enumeration (CWE) database or Common Vulnerabilities and Exposures (CVE) database in remediating flaws discovered in organizational systems.

Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types of remediation.

[SP 800-40] provides guidance on patch management technologies.

WPI Wisconsin Procurement Institute
AN APEX ACCELERATOR
APEX ACCELERATORS

3.14 Basics

Vulnerability Scanning

Alerts

IDS/AV

Log Review

Controls & Objectives

1 — Understanding the Controls

2 — Controls & Objectives

3 — Documentation & Evidence

3.13.1	**SECURITY REQUIREMENT** Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.1[a] *the external system boundary is defined.*
	3.13.1[b] *key internal system boundaries are defined.*
	3.13.1[c] *communications are monitored at the external system boundary.*
	3.13.1[d] *communications are monitored at key internal boundaries.*
	3.13.1[e] *communications are controlled at the external system boundary.*
	3.13.1[f] *communications are controlled at key internal boundaries.*
	3.13.1[g] *communications are protected at the external system boundary.*
	3.13.1[h] *communications are protected at key internal boundaries.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; enterprise security architecture documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities]. Test: [*SELECT FROM:* Mechanisms implementing boundary protection capability].

3.13.1 – Meeting the Controls

NETWORK DIAGRAM

ACCESS CONTROL LIST

CONFIG FILES

3.13.1[a] the external system boundary is defined.

3.13.1[b] key internal system boundaries are defined.

3.13.1[c] communications are monitored at the external system boundary.

3.13.1[d] communications are monitored at key internal boundaries.

3.13.1[e] communications are controlled at the external system boundary.

3.13.1[f] communications are controlled at key internal boundaries.

3.13.1[g] communications are protected at the external system boundary.

3.13.1[h] communications are protected at key internal boundaries.

Documentation of Policy and Architecture.

Intentions and allowances listed.

Validation of technical implementation.

3.13.3	SECURITY REQUIREMENT Separate user functionality from system management functionality.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.3[a] *user functionality is identified.*
	3.13.3[b] *system management functionality is identified.*
	3.13.3[c] *user functionality is separated from system management functionality.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System and communications protection policy; procedures addressing application partitioning; system design documentation; system configuration settings and associated documentation; system security plan; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer]. Test: [*SELECT FROM:* Separation of user functionality from system management functionality].

3.13.3 – Meeting the Controls

Account Authorization Policy

3.13.3[a] user functionality is identified.

3.13.3[b] system management functionality is identified.

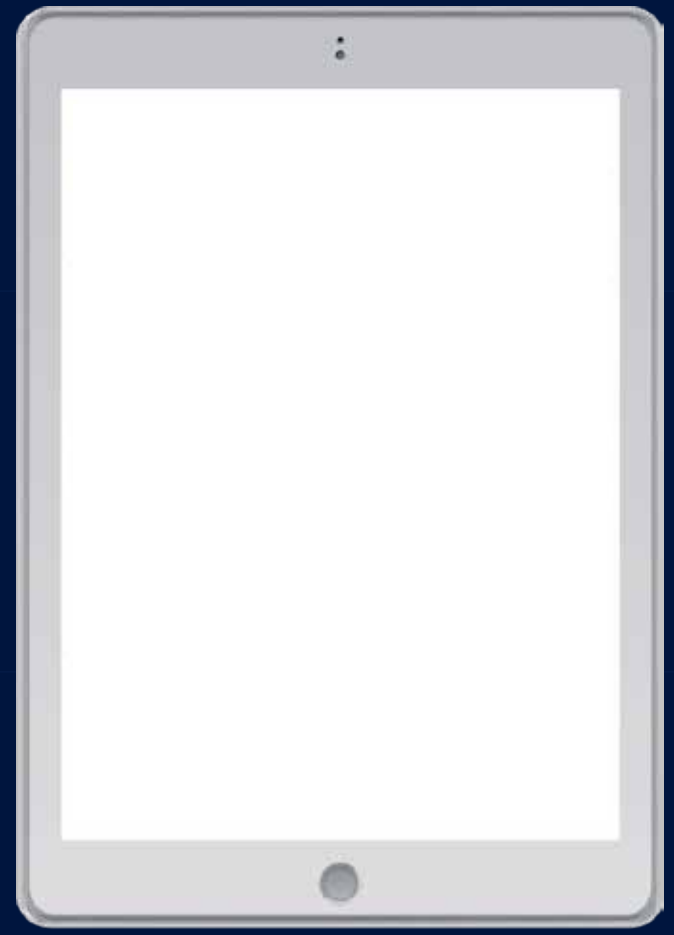
3.13.3[c] user functionality is separated from system management functionality.

AD Users Review (Security Group Review)

Should be previously established in Access Control Family.

Expanded here to include not only domain but boundary/cloud users.

System and Communications



Prior Documentation

- Network Diagram
- Access Control Policy
- IT Security Policies
- Log Management Policy

Technical Artifacts

- Screenshots of Configurations
- CFG Files From Boundary Devices
- FIPS / FEDRAMP Equivalent Encryption Means

Updating Documentation

- SSP Implementation Statement Update
- Review All Supporting Documentation
- Review All Encryption Standards

3.14.1	**SECURITY REQUIREMENT** Identify, report, and correct system flaws in a timely manner.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.1[a] *the time within which to identify system flaws is specified.*
	3.14.1[b] *system flaws are identified within the specified time frame.*
	3.14.1[c] *the time within which to report system flaws is specified.*
	3.14.1[d] *system flaws are reported within the specified time frame.*
	3.14.1[e] *the time within which to correct system flaws is specified.*
	3.14.1[f] *system flaws are corrected within the specified time frame.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility]. Test: [*SELECT FROM:* Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates].

3.14.1 – Meeting the Controls

Vulnerability Scanning Process

3.14.1[a] the time within which to identify system flaws is specified.

3.14.1[b] system flaws are identified within the specified time frame.

3.14.1[c] the time within which to report system flaws is specified.

3.14.1[d] system flaws are reported within the specified time frame.

3.14.1[e] the time within which to correct system flaws is specified.

3.14.1[f] system flaws are corrected within the specified time frame.

Validation Process

AV Scanning Policy

Touches upon programs already established but now enforced through validation.

3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.2[a]	*designated locations for malicious code protection are identified.*
	3.14.2[b]	*protection from malicious code at designated locations is provided.*
3.14.3	**SECURITY REQUIREMENT** Monitor system security alerts and advisories and take action in response.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.3[a]	*response actions to system security alerts and advisories are identified.*
	3.14.3[b]	*system security alerts and advisories are monitored.*
	3.14.3[c]	*actions in response to system security alerts and advisories are taken.*
3.14.4	**SECURITY REQUIREMENT** Update malicious code protection mechanisms when new releases are available.	
	ASSESSMENT OBJECTIVE *Determine if malicious code protection mechanisms are updated when new releases are available.*	

3.14.2 – Meeting the Controls
3.14.3 & 3.14.4

AV Management Process Defined

3.14.2[a] designated locations for malicious code protection are identified.

3.14.2[b] protection from malicious code at designated locations is provided.

3.14.3[a] response actions to system security alerts and advisories are identified.

3.14.3lb] system security alerts and advisories are monitored.

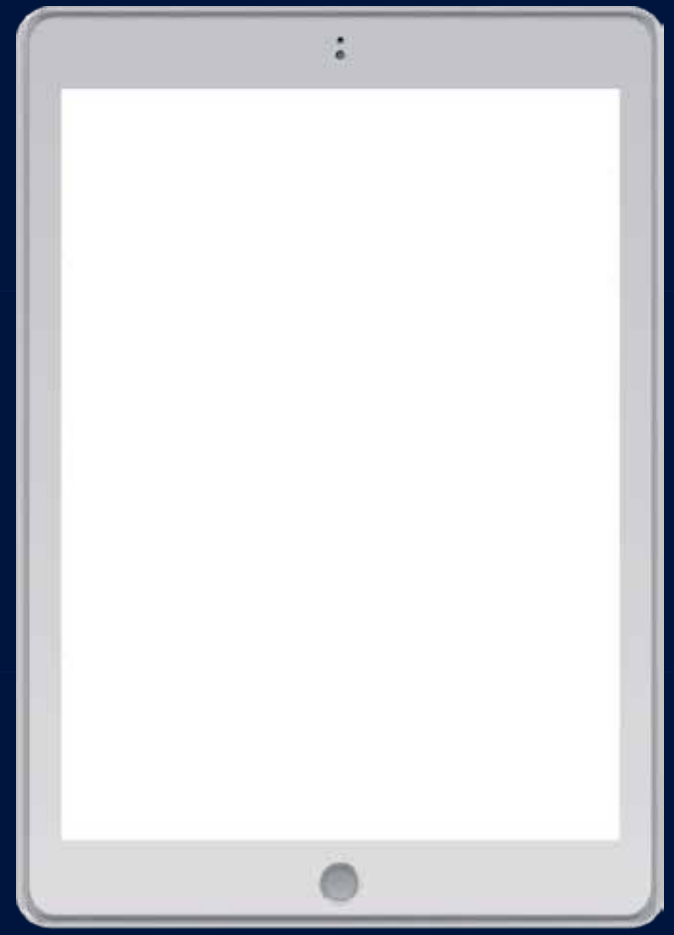
3.14.3[c] actions in response to system security alerts and advisories are taken.

3.14.4[a] determine if malicious code protection mechanisms are updated when new releases are available.

Screenshots

Commonly AV suites provide much of this as an integrated part of their solution. Capturing configuration screenshots and showing process of review/mitigation of AV Scan Results are necessary.

System and Information



Vulnerability Scanning

- In Place
- Process Documented
- Mitigations Performed
- Review / Validation

Antivirus

- Installed
- Process (often automated) defined in policy or procedural document
- Results Validated Consistently

Additional Monitoring

- Security Alerts established through system.
- Process of response / review of alerts in place.
- IDS, AV, and Vulnerability Scanning Tools controlled and defined.

Documentation & Evidence

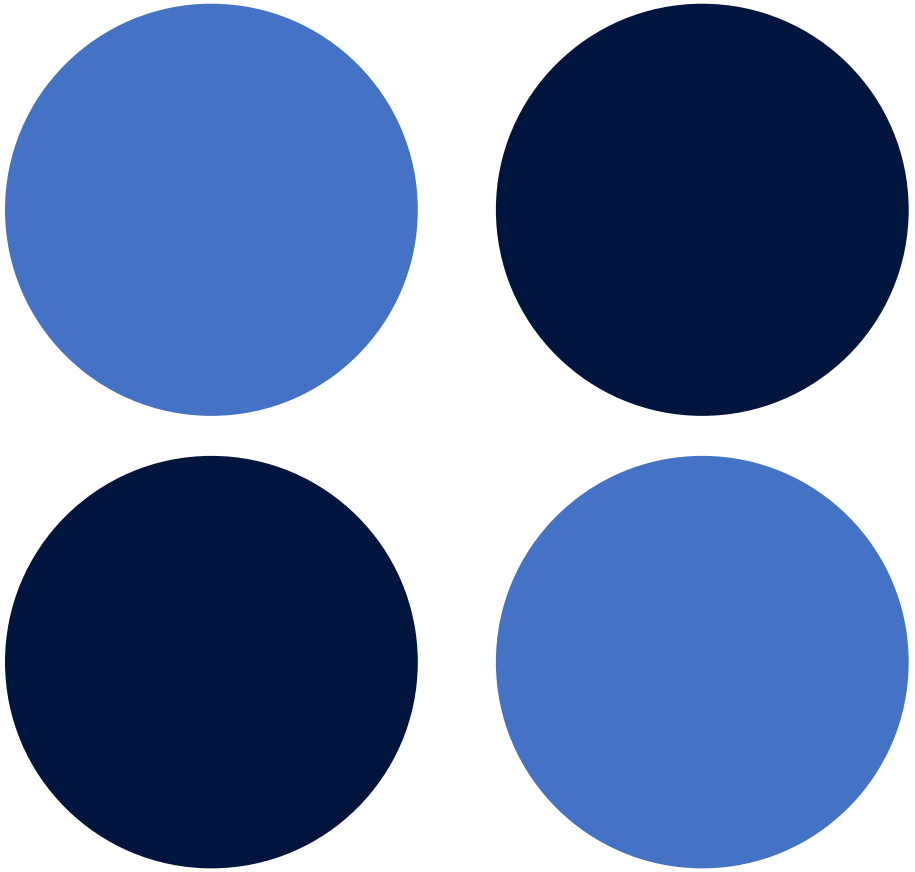
1 — Understanding the Controls

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.

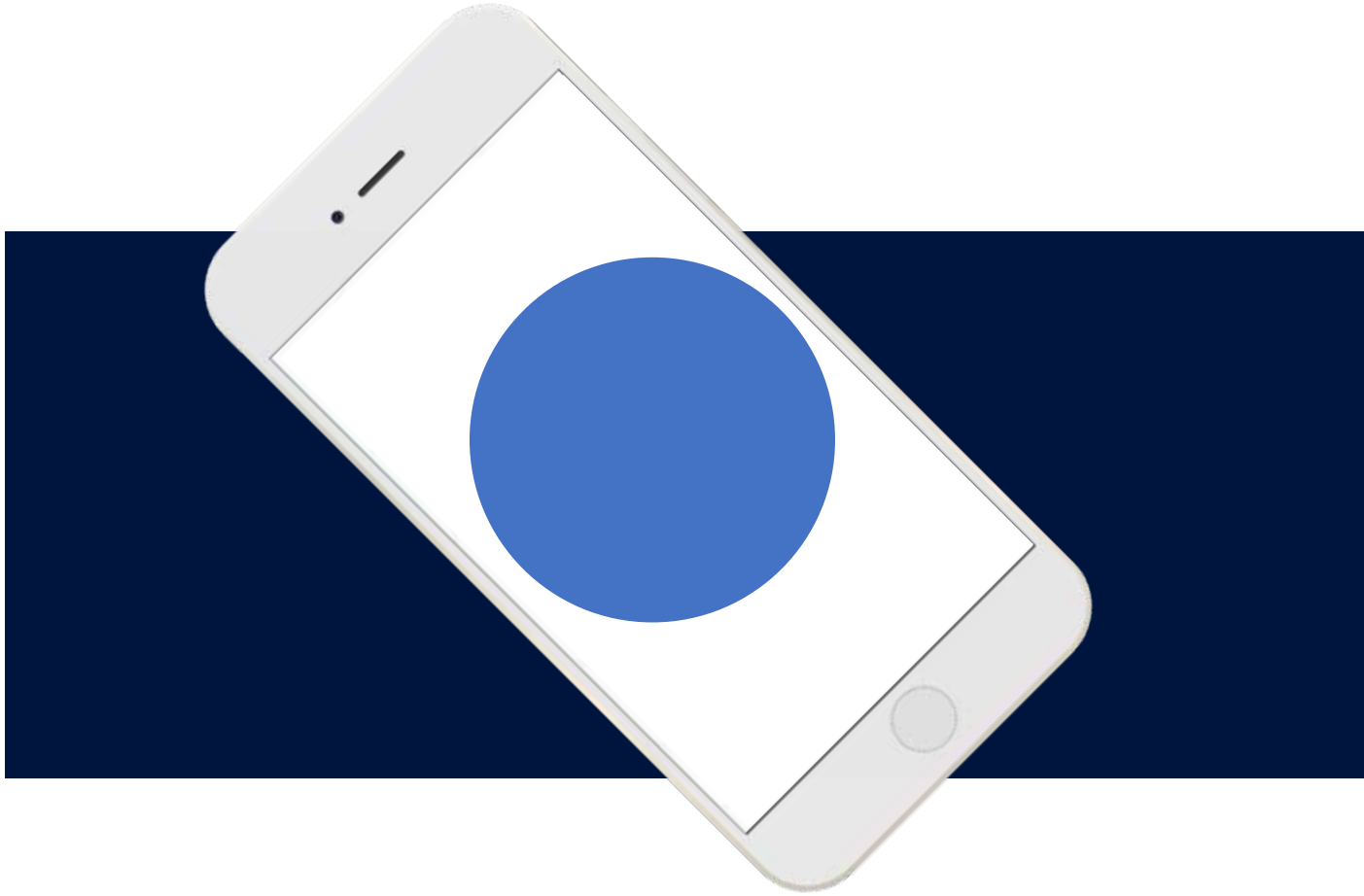
Reviews
are periodically conducted, tracked, and summarized.

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR



Wisconsin Procurement Institute

APEX ACCELERATORS

Cyber Friday:

NIST SP 800.171 – 3.13 System and Communications Protection and 3.14 System and Information Integrity

November 9| 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

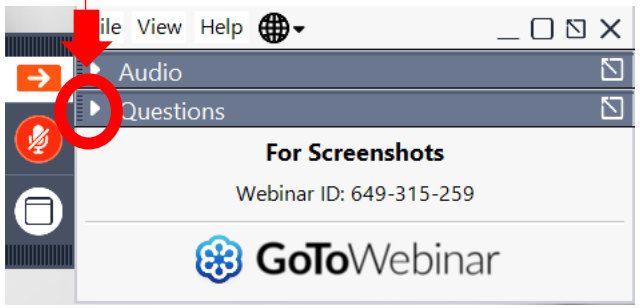
THANK YOU!

Wisconsin Procurement Institute

NCMA WISCONSIN

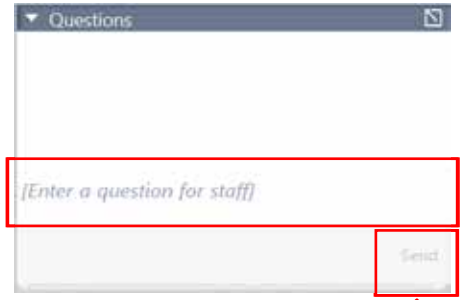
OPENING THE QUESTIONS BOX

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.

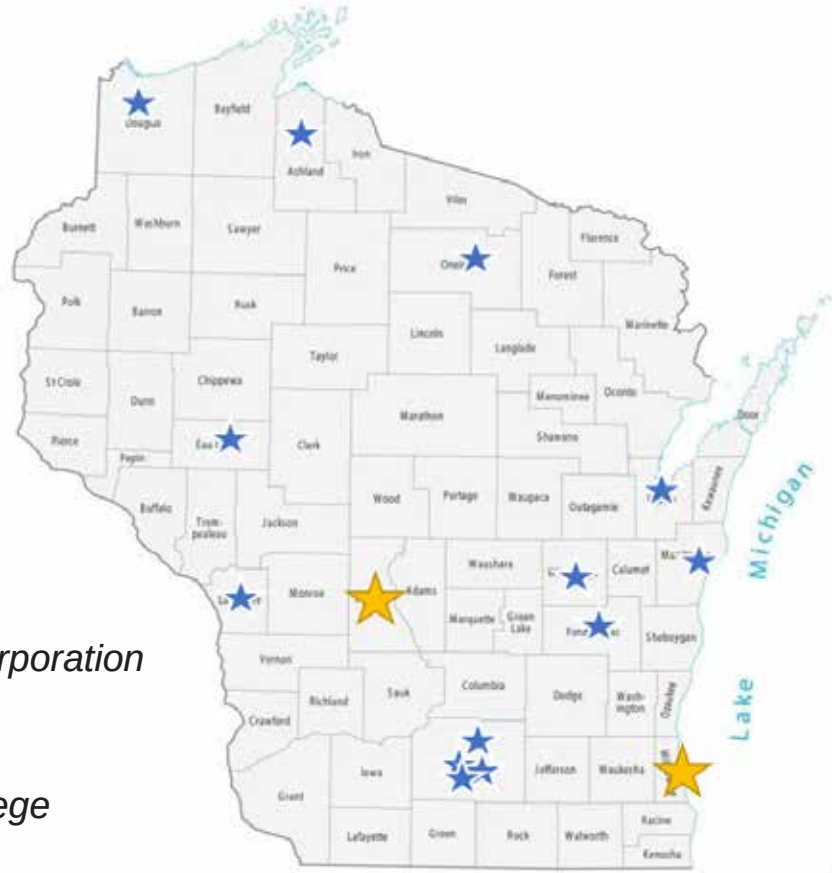
WPI provides services to all of Wisconsin's 72 counties

- 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

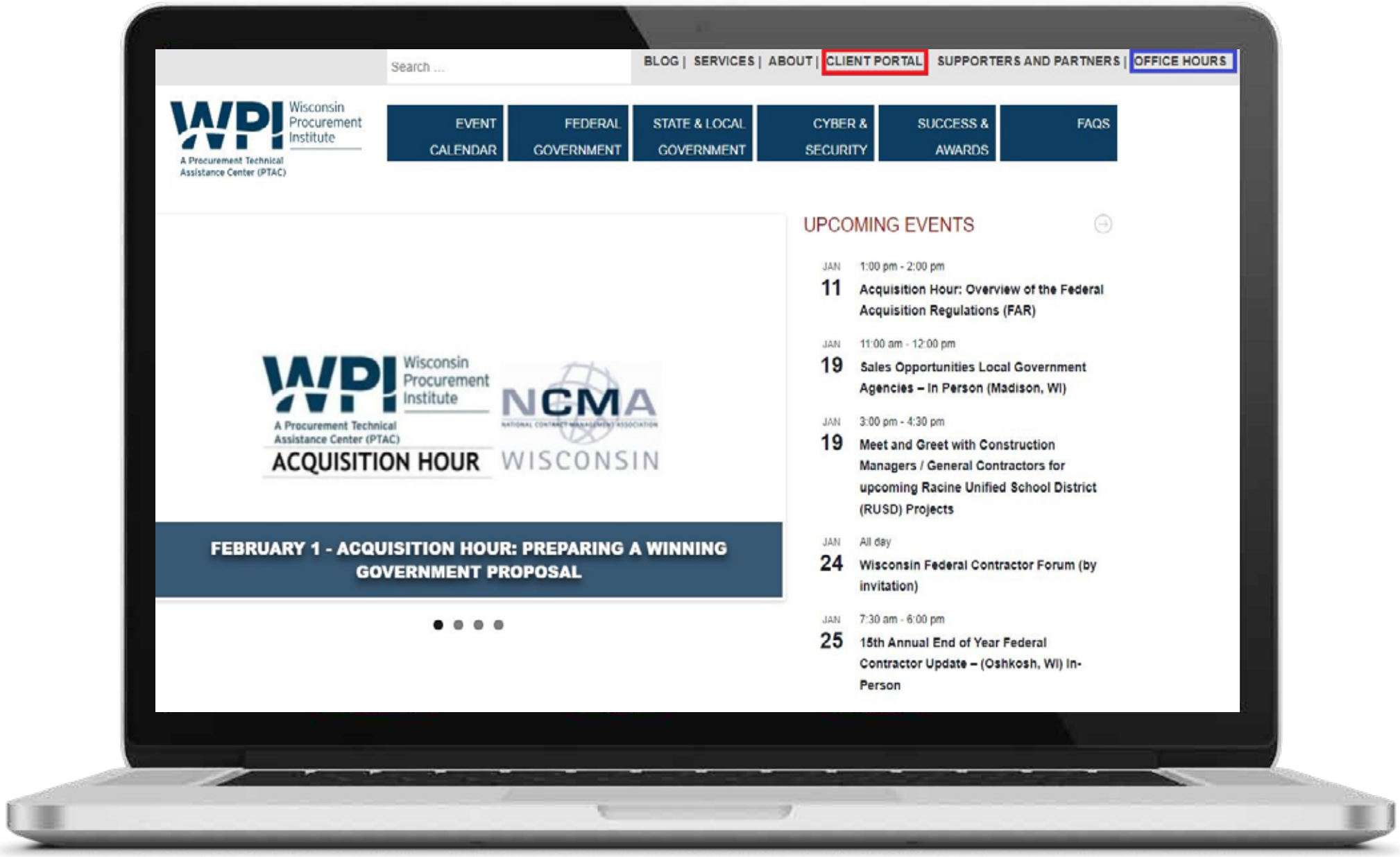
WPI OFFICE LOCATIONS

- **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



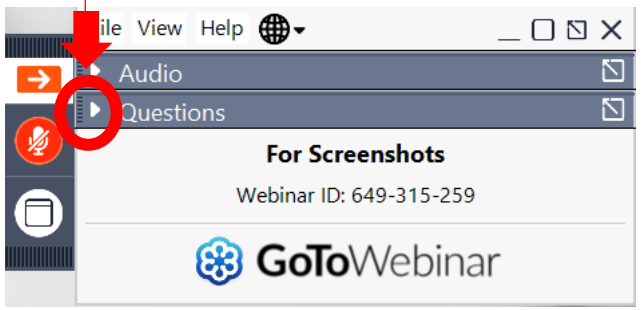
WPI Wisconsin Procurement Institute APEX

NCMA WISCONSIN

QUESTIONS?

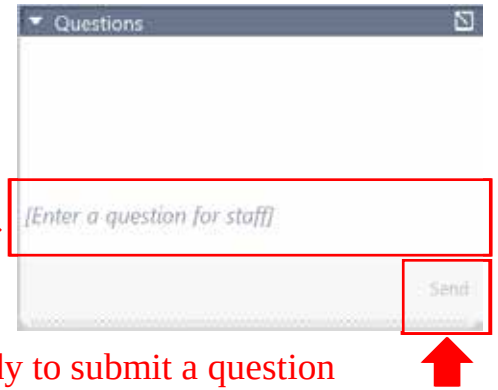
OPENING THE QUESTIONS BOX

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

November 9, 2023

Registration Now Open

NCMA WISCONSIN

WPI Wisconsin Procurement Institute

APEX ACCELERATORS

Announcing 2024

Evening FAR Sessions

January 30 – March 19

Wispro.org/Events

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

November 9, 2023

SURVEY

Wisconsin Procurement Institute

November 9, 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