Wisconsin Procurement Institute

AN APEX ACCELERATOR

APEX ACCELERATORS

CYBER FRIDAY: SYSTEM SECURITY PLAN AND PLAN OF ACTION AND MILESTONES CONSTRUCTION

February 24, 2023 @ 11:00 am - Noon

Presented by Matt Frost, WPI

Wisconsin Procurement Institute

AN APEX ACCELERATOR

Cyber Friday

Webinar Etiquette

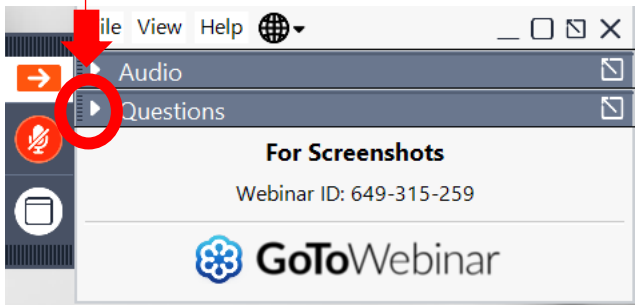
PLEASE

- 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!

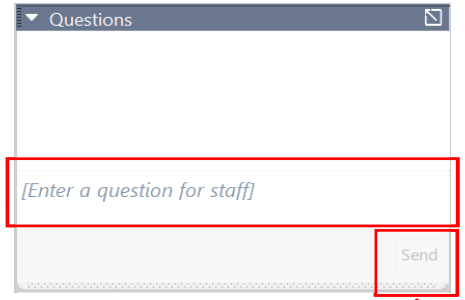
OPENING THE QUESTIONS BOX

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

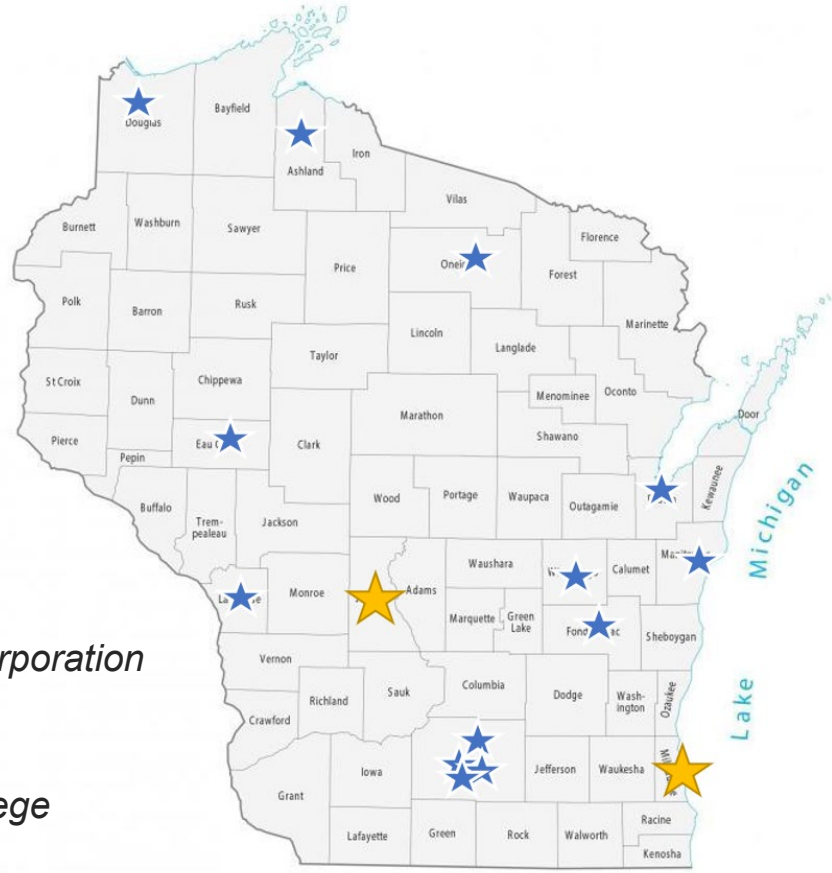
The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides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

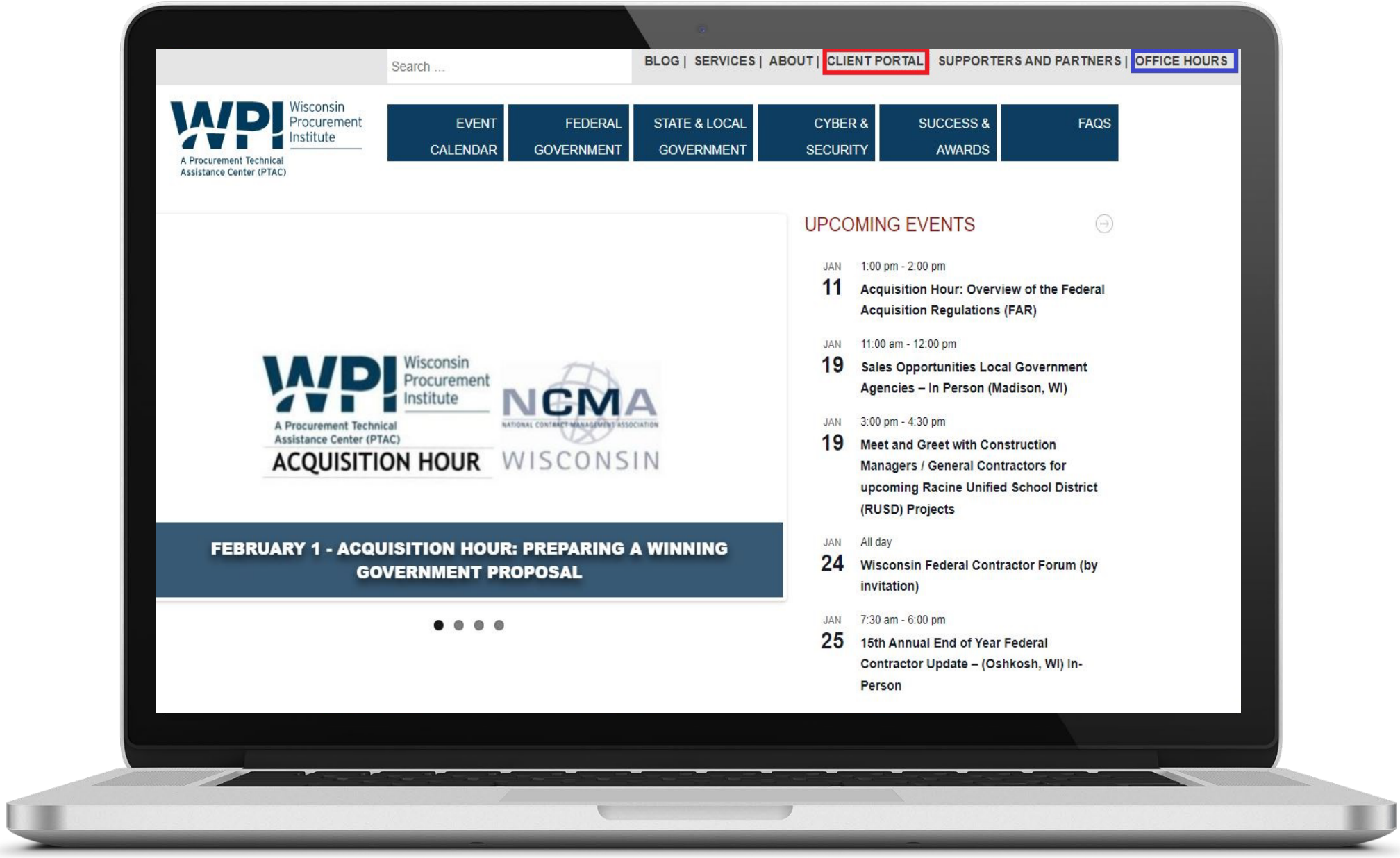
More about WPI

- 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*

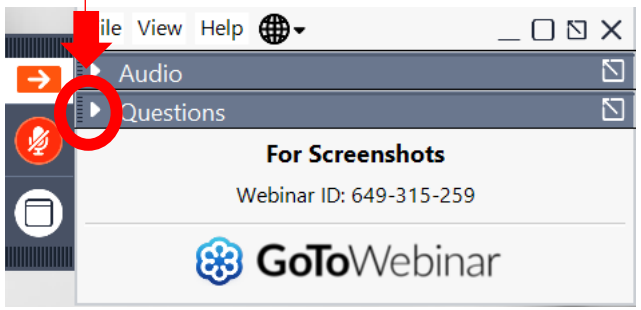



Search ...
BLOG | SERVICES | ABOUT | CLIENT PORTAL SUPPORTERS AND PARTNERS | OFFICE HOURS
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
CYBER & SECURITY
SUCCESS & AWARDS
FAQS
Wisconsin Procurement Institute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

QUESTIONS?

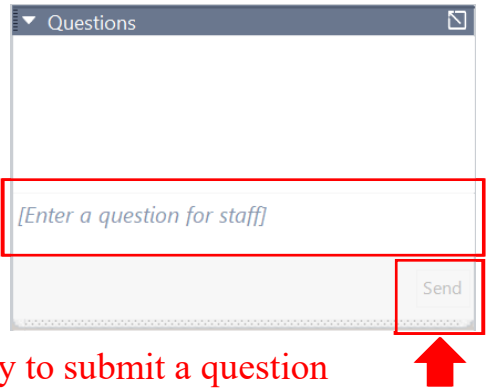
OPENING THE QUESTIONS BOX

Click here to access within the Control Panel



USING THE QUESTIONS BOX

Type questions here at any time during a presentation

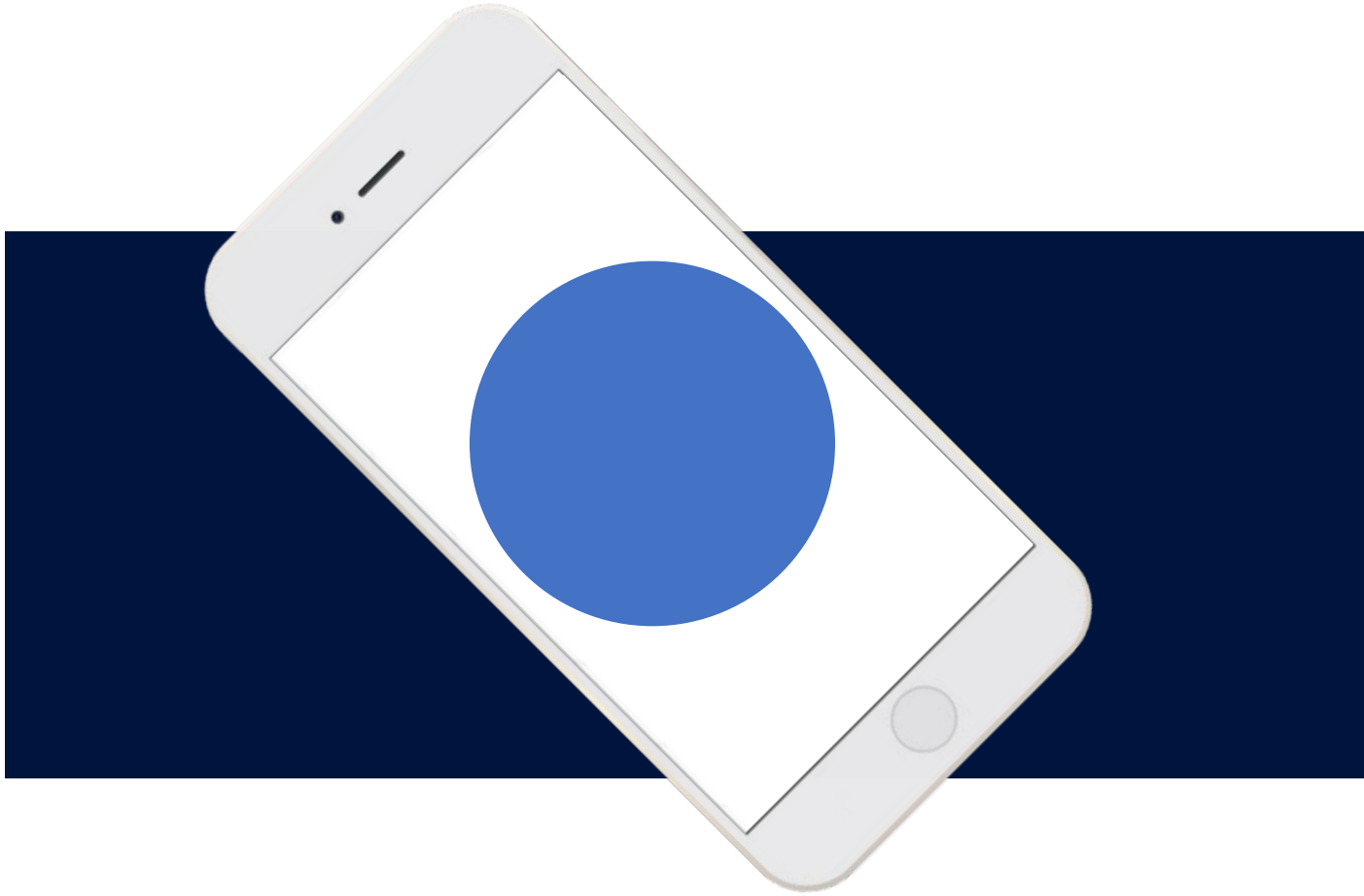


Click Send when ready to submit a question

System Security Plans & Plans of Action and Milestones

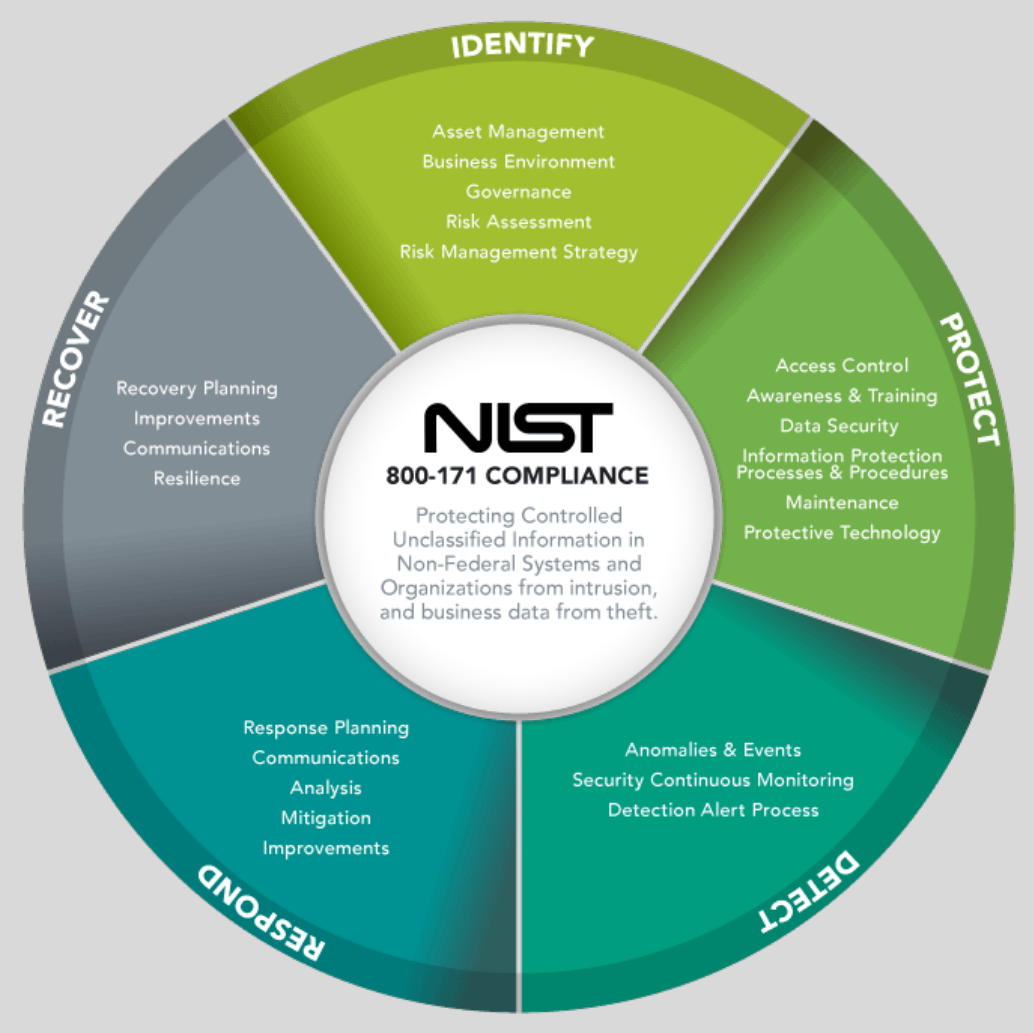
Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – February 10th, 2023

DFARS 252.204-7019



- ❑ The Contractor shall provide adequate security on all covered contractor information systems.
- ❑ The contractor shall implement NIST SP 800-171.

NIST SP 800-171r2

Chapter 3: Page 9 NIST SP 800-171r2

Nonfederal organizations describe, in a system security plan, how the security requirements are met or how organizations plan to meet the requirements and address known and anticipated threats. The system security plan describes: the system boundary; operational environment; how security requirements are implemented; and the relationships with or connections to other systems.

Nonfederal organizations develop plans of action that describe how unimplemented security requirements will be met and how any planned mitigations will be implemented.

Organizations can document the system security plan and the plan of action as separate or combined documents and in any chosen format.

DFARS 252.204-7012

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 System Security Plan

NIST SP 800-171

1 — SSP

2 — POAM

3 — APPROVE

NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST Special Publication 800-18 Revision 1

1

NIST Special Publication 800-18
Revision 1
Guide for Developing Security Plans
for Federal Information Systems

NIST SP 800-171r2

2

NIST Special Publication 800-171r2
Protecting Controlled Unclassified
Information in Nonfederal Systems
and Organizations

NIST SP 800-171A

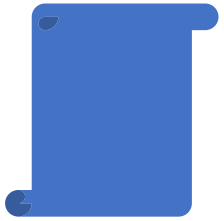
3

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

System Security Plan

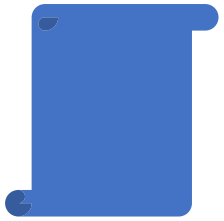
- Living Document
- Plan of Actions and Milestones (POAM)
- Defines Categorization for the Information System
- Provides an Overview of the Security Requirements for the information system
- Describes the Security Controls in place for those requirements

Organization of the System Security Plan



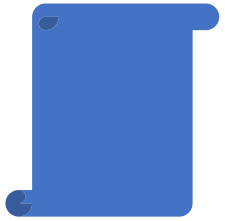
Section 1

Includes background information relevant to the system security planning process, target audience,, and a description of the roles and responsibilities related to the development of SSPs.



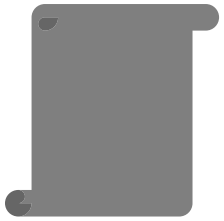
Section 2

Discusses how agencies should analyze their information system inventories in the process of establishing system boundaries. It also discusses identification of common security controls and scoping guidance.



Section 3

Provides additional points or notes, includes a history of versions, and can include an appendix of definitions or signatures of approving officials.



Appendixes/Attachments

Network Diagrams, Hardware Inventory, Software Inventory, Business Process Flow Diagram, Supporting Process Documentation, POAM

System Information

System Name and Identifier

Each system should be assigned a name and unique identifier. This should remain the same throughout the life of the system.

System Categorization

System must be categorized in accordance using FIPS 199.

NIST SP 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories

ROLES AND RESPONSIBILITIES

The necessary roles and requisite responsibilities attached to each roles.

FIPS 199

1. System Identification

1.1	System Name	Test Company	☐
1.1.1	System Categorization	LOW	☐
1.1.2	System Unique Identifier	TC System	☐

1.2 Responsible Organization

1.2.1	Company Name	The Test Company's Security Team	☐
1.2.2	Address		☐
1.2.3	Phone		☐

FIPS 199

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Assigning Roles

CHIEF INFORMATION OFFICER

Agency Official responsible for developing and maintaining an agency-wide information security program.

- ❑ Develops and Maintains information security policies, procedures, and control techniques
- ❑ Manages the identification, implementation, and assessment of common security controls
- ❑ Ensures personnel with responsibilities are trained
- ❑ Assists senior officials with their responsibilities
- ❑ Identifies and coordinates common security controls

INFORMATION SECURITY OFFICER

Agency Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system.

- ❑ Develops the SSP in coordination with IO's, System Administrator, CIO, and End Users
- ❑ Maintains the SSP and ensures that the system is deployed and operated according to requirements.
- ❑ Updates SSP when changes occur
- ❑ Assists in the identification, implementation, and assessment of the controls.

INFORMATION OWNER

Agency Official with statutory or operational authority for specificied information and responsibility for establishing the controls.

- ❑ Establishes the rules for appropriate use and protection of information.
- ❑ Provides input regarding the security requirements and security controls.
- ❑ Decides who has access to the information system and what types of privileges or access rights.
- ❑ Assists in the identification and assessment of controls.

AUTHORIZING OFFICIAL

Senior Management Official with the authority to formally assume responsibility for information system.

- ❑ Approvies SSPs
- ❑ Authorizes operation of Information System
- ❑ Denies authorization to operate the information system if an unacceptable risk exists.

FIPS 199

1.3 Information Owner

1.3.1	Name		☐
1.3.2	Title		☐
1.3.3	Office Address		☐
1.3.4	Work Phone		☐
1.3.5	E-Mail Address		☐

1.4 System Security Officer

1.3.1	Name		☐
1.3.2	Title		☐
1.3.3	Office Address		☐
1.3.4	Work Phone		☐
1.3.5	E-Mail Address		☐

1.5 General Description/Purpose of System

1.5.1	Description	Test Company's IT For CUI	☐
1.5.2	Number of Users/Privileged Users		☐
1.5.3	Description of Information		☐

Scoping the Information System

System Boundaries

- ❑ Under the same direct management control
- ❑ Have the same function or objective
- ❑ Same characteristics or security needs
- ❑ Reside in the same general operating environment

Major Applications

- ❑ Requires special attention due to importance to mission
- ❑ High Development, Operating, or maintenance costs
- ❑ Can compromise multiple programs, hardware, software, and telecom components.
- ❑ Explains Cyber Risks

General Support Systems

- ❑ Interconnected set of resources under the same management control that shares common functionality.
- ❑ LAN, Backbone, Com Network, Data Processing Center, etc.

Minor Applications

- ❑ Typically secured by system in which it resides
- ❑ Of low importance or use
- ❑ May or may not interact with CUI

FIPS 199

2. System Environment

Network Topology Drawing ☐

Network Topology Narrative/Business Process Flow ☐

2.1 Listing of Hardware		☒
2.2 Listing of Software		☐
2.3 Hardware/Software Maintenance and Ownership		☒

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

3.1.3[a] information flow control policies are defined.	☒
Information Flow Control Policies are defined clearly in the Business Process Flow (addendum.)	
3.1.3[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.	☒
Boundaries devices restrict unauthorized access to the information system. Use of information system is governed by acceptable use policy. Consequences of operating outside of designated policy are managed by disciplinary process detailed in employee handbook. Enforcement mechanisms include Active Directory, Boundary Firewall, Endpoint Management Utility, Employee Handbook, and Acceptable Use Policy.	
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.	☒
Networks and Individuals (by role) are identified in the Business Process Flow. Additional endpoint/devices are defined within Network Topology Diagram and Hardware Inventory. Sources for information outside of the network are defined in the Business Process Flow Diagram.	
3.1.3[d] authorizations for controlling the flow of CUI are defined.	☒
All authorizations regarding the control of the flow of CUI are defined within the acceptable use policy and system baseline documentation addendums.	
3.1.3[e] system access is limited to processes acting on behalf of authorized users.	☒
Service Accounts Alpha and Bravo access CUI only on the behalf of authorized users through the use of ALPHABRAVO Application and this process is identified in the Business Process Flow Diagram. ALPHABRAVO Application is listed on the software inventory.	
3.1.3[f] approved authorizations for controlling the flow of CUI are enforced.	☒
Failure to operate within the parameters established by Test Company will result in strict enforcement under the disciplinary process outlined in the Employee Handbook. Additionally, Active Directory and Boundary Firewall enforce digital authorization to ensure access is restricted to those employees that have been approved and accepted the terms of acceptable use.	

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

Notes:

The Plan of Action and Milestones

NIST SP 800-171

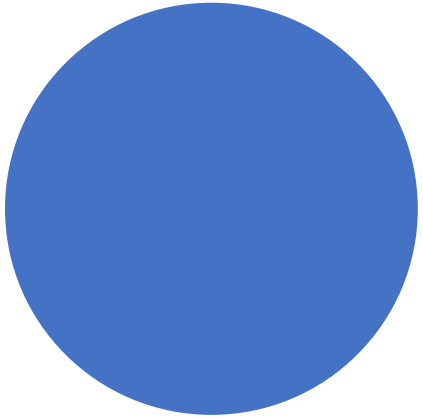
1 — SSP

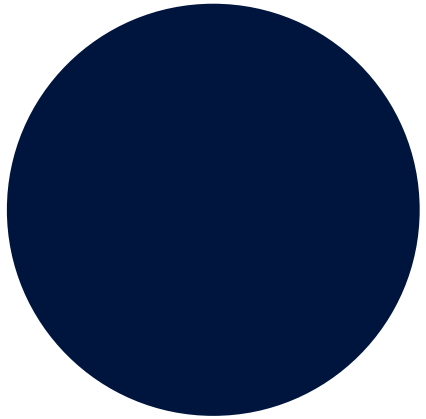
2 — POAM

3 — APPROVE

Plan of Action and Milestones

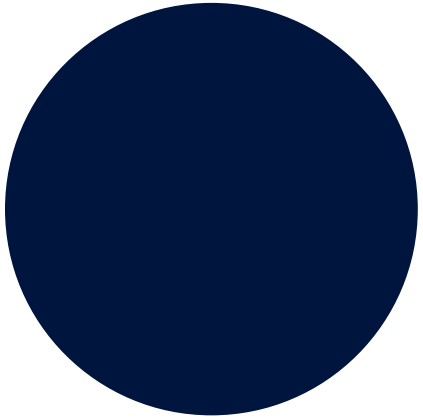
Tasks that need to be accomplished

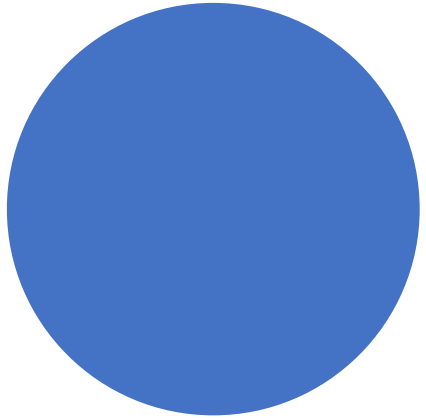




Milestones for meeting the tasks

Resources required to accomplish the elements of the plan





Scheduled completion dates for the milestones

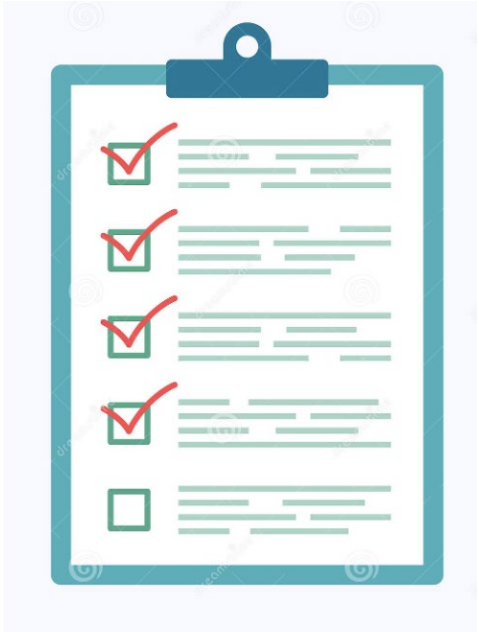
NIST Control Number	Control	Responsible Office	Scheduled Completion Date	Milestones with Interim Completion Dates
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).			
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.			
3.1.3	Control the flow of CUI in accordance with approved authorizations.	ISO - John Johnston	Jun-23	Draw Business Process Flow, Update Employee Handbook, Draft Acceptable Use Policy. Review Service Accounts and ensure Alpha and Bravo account activity is correctly logged.

The Self-Assessment Process

NIST SP 800-171

1 — PREPARE

2 — ASSESS



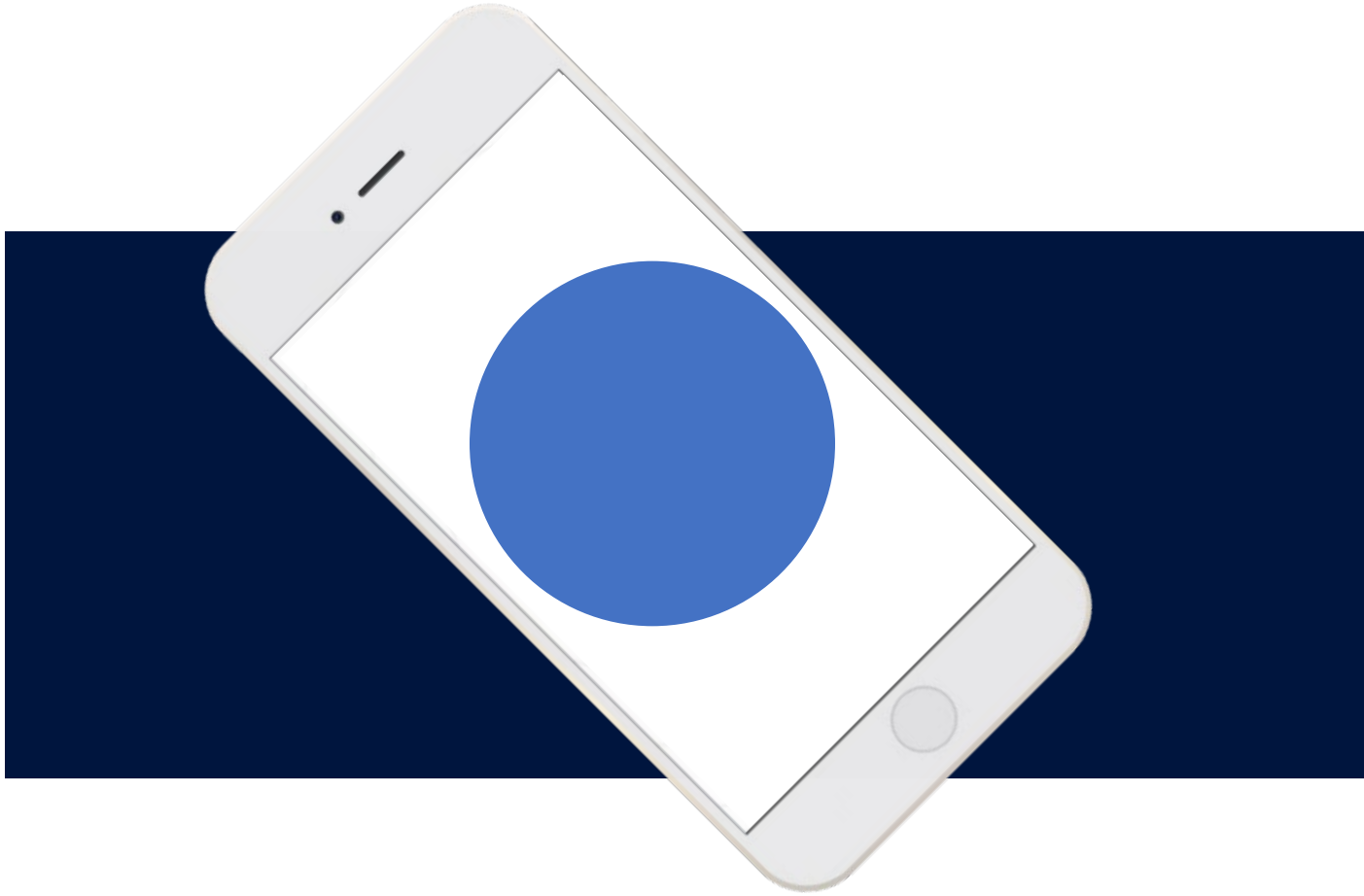
3 — APPROVE

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR



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

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 24, 2023

SURVEY

Wisconsin Procurement Institute
AN APEX ACCELERATOR

February 24, 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