Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:

Building a CMMC Program: 3.1.1 Access Control Lists, Account Request Documentation, and Acceptable User Policies

May 17| 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

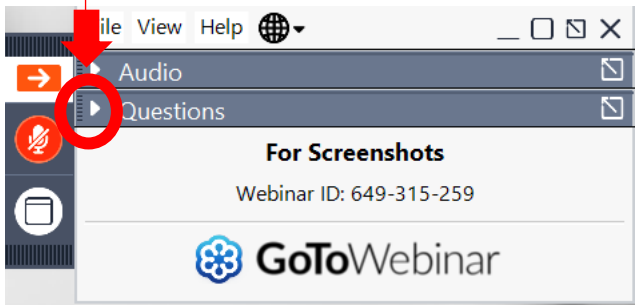
PLEASE

- 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!

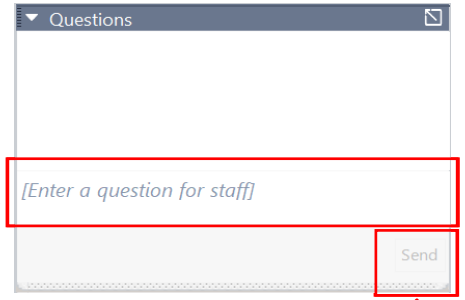
OPENING THE QUESTIONS BOX

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

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

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.

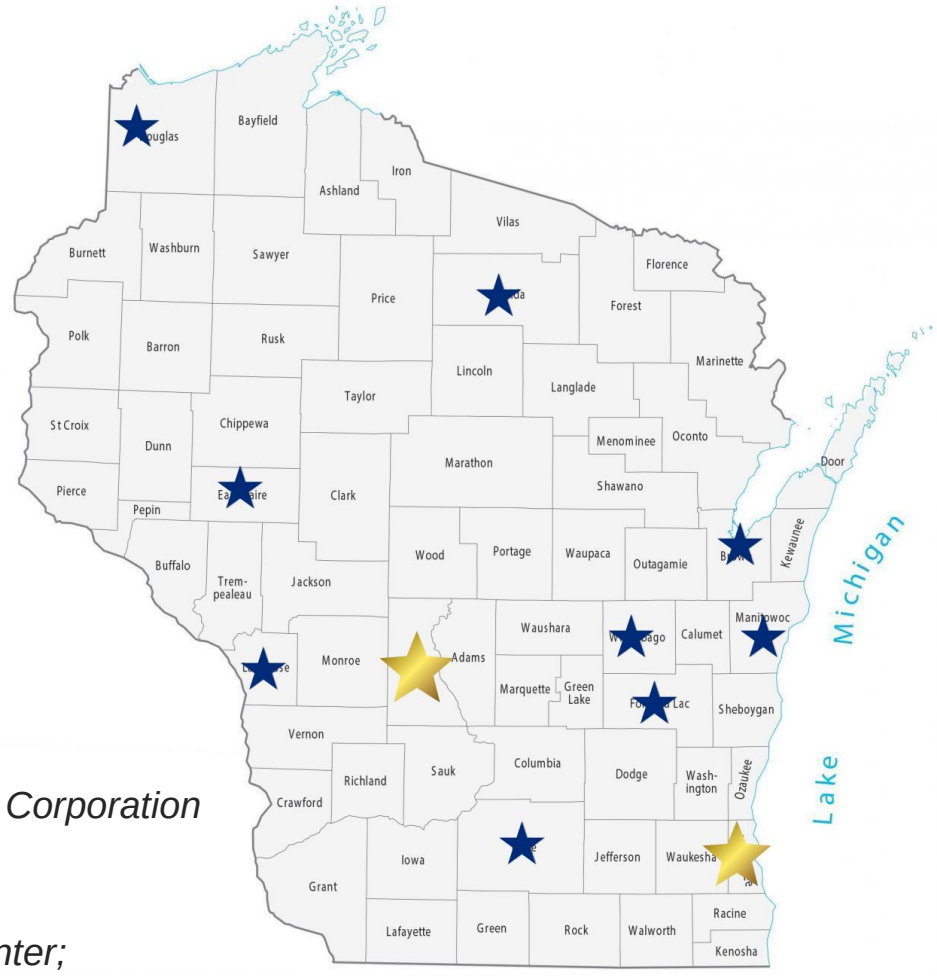
WPI provides services to all of Wisconsin's 72 counties

- 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……

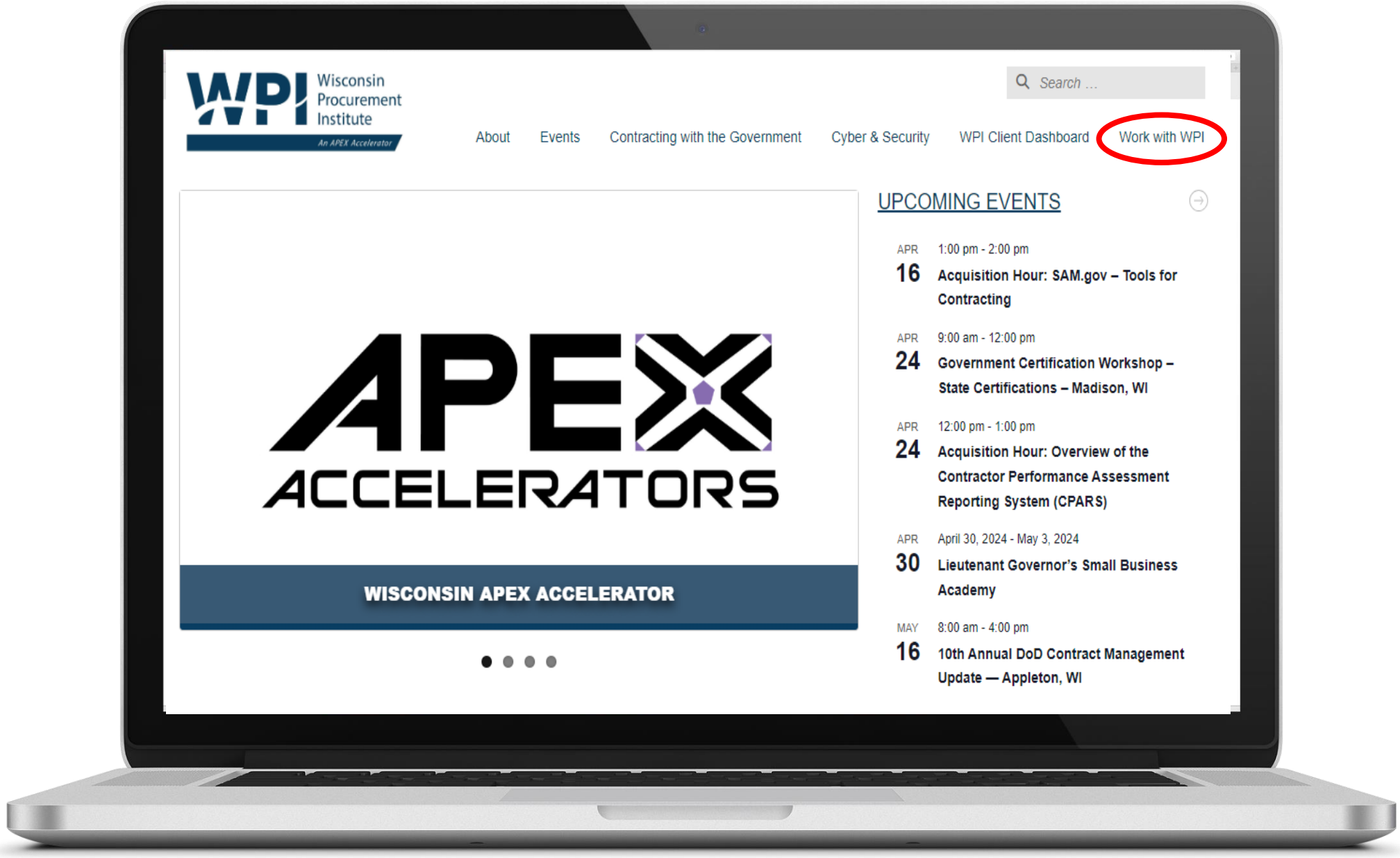
www.wispro.org

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)*
- **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*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*



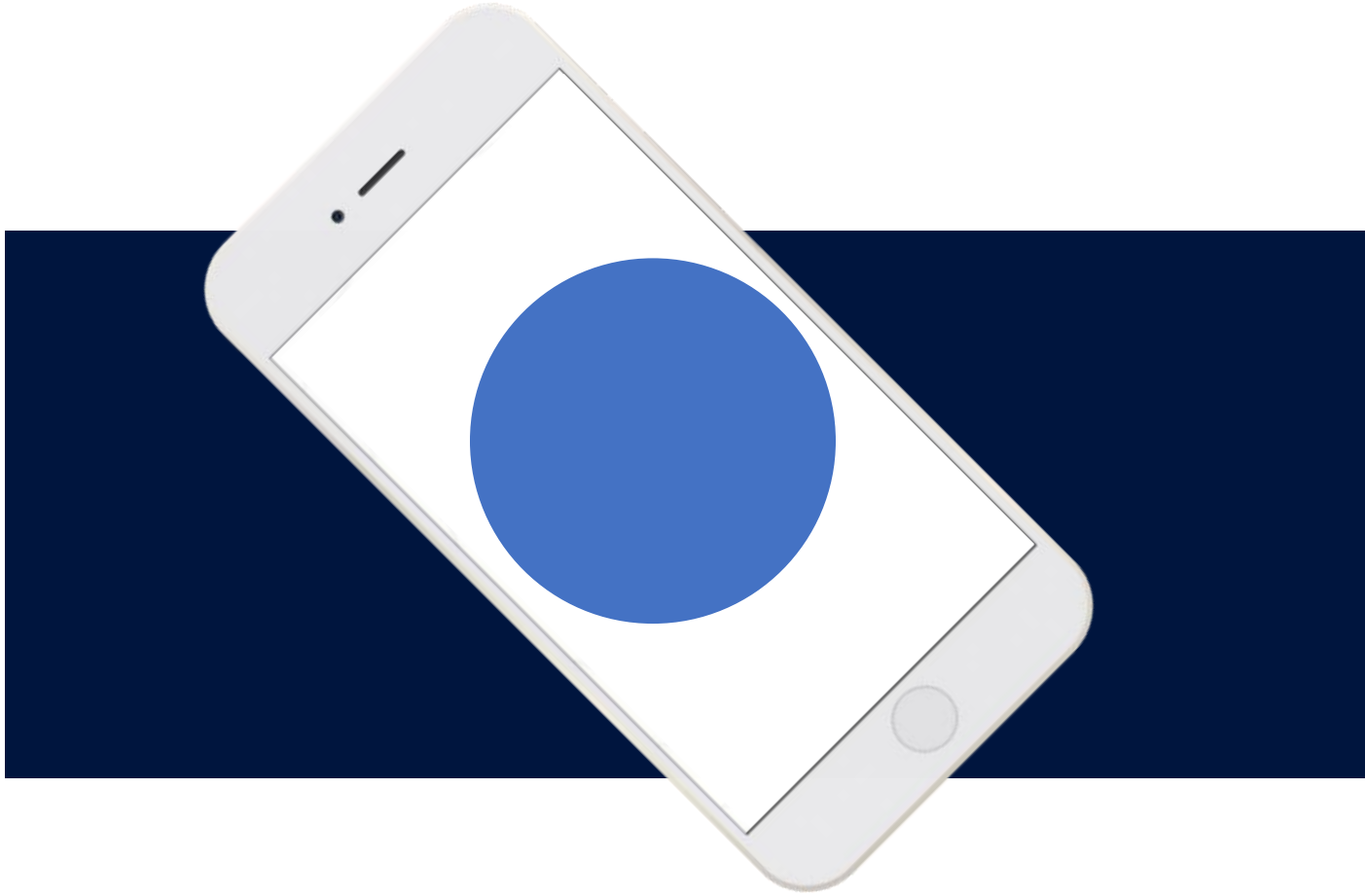
Wisconsin Procurement Institute
An APEX Accelerator


WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

Documentation for NIST SP 800-171r2 Controls

Wisconsin Procurement Institute

AN APEX ACCELERATOR



CYBER FRIDAY SESSIONS – May 17th, 2024

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.

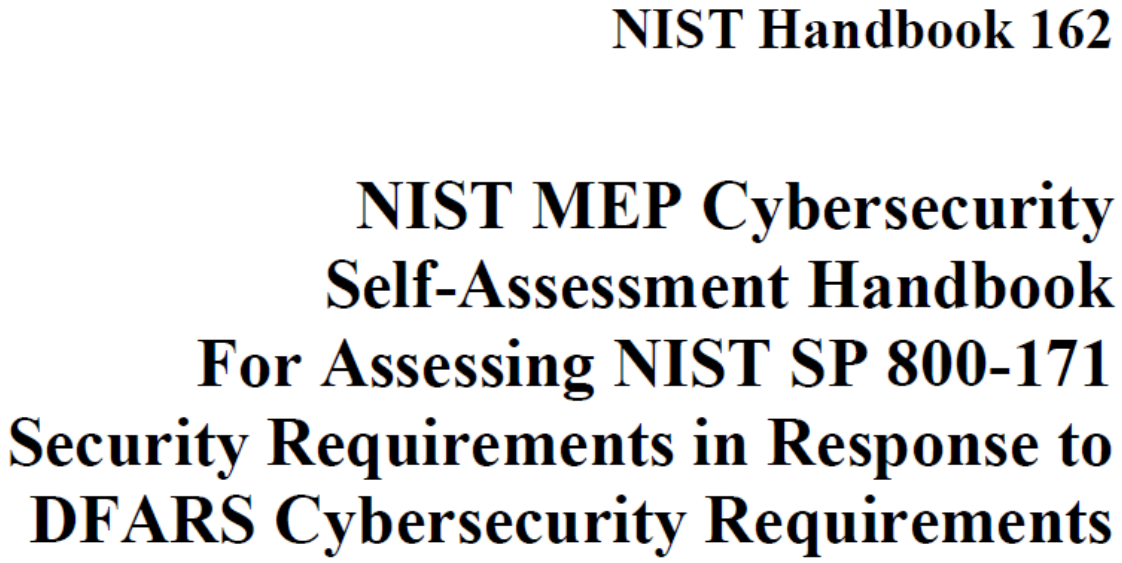
DFARS 252.204-7021

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 800-18r1

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

Reading the Controls

NIST SP 800-171

1

Account Management Policy

2

Acceptable Use Policy

3

Access Control Policy

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.1[a] *authorized users are identified.*
	3.1.1[b] *processes acting on behalf of authorized users are identified.*
	3.1.1[c] *devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d] *system access is limited to authorized users.*
	3.1.1[e] *system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f] *system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Section 1: Requestor Information

Name	
Position	
Department	
Phone Number	
Email Address	

Section 2: Type of Request

- New Account
- Modify Account
- Deactivate Account

Section 3: Compliance and Security

Justification for Access:

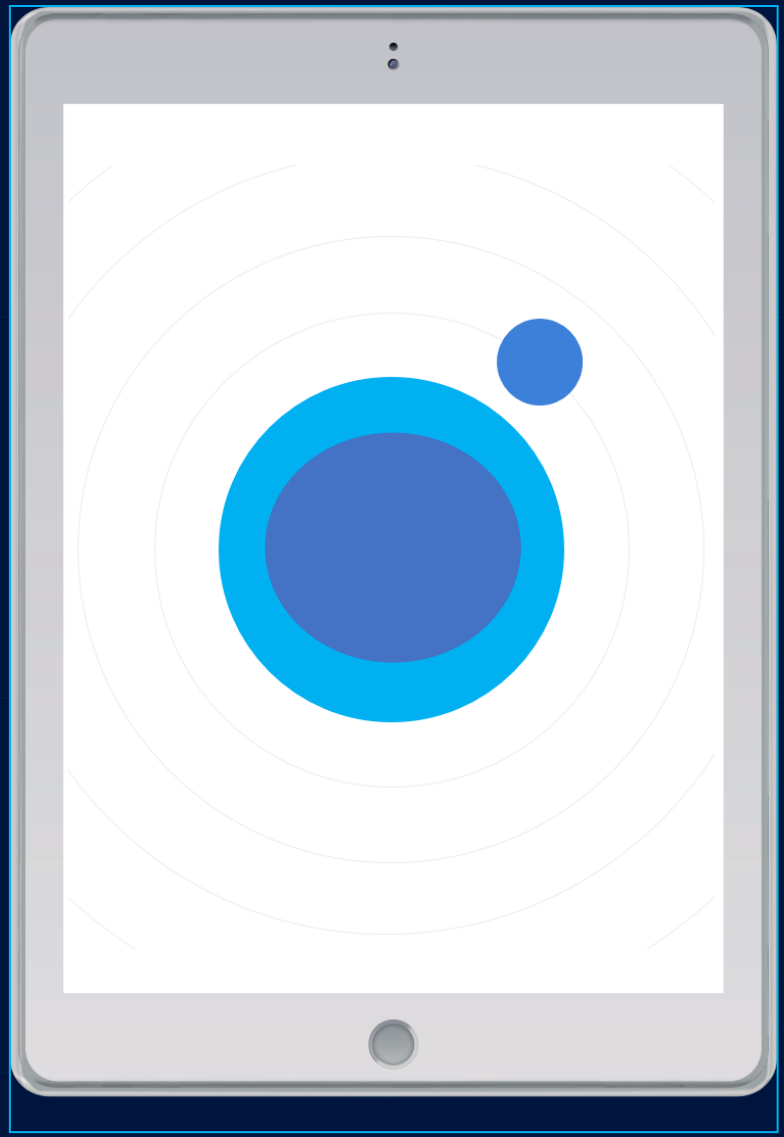
_____

_____

Multi-Factor Authentication (MFA) Required: [_] Yes [_] No

Security Training Completed: [_] Yes [_] No

Account Request Form



Section 4: Authorizations

Immediate Supervisor

Name	
Title	
Signature	
Date	

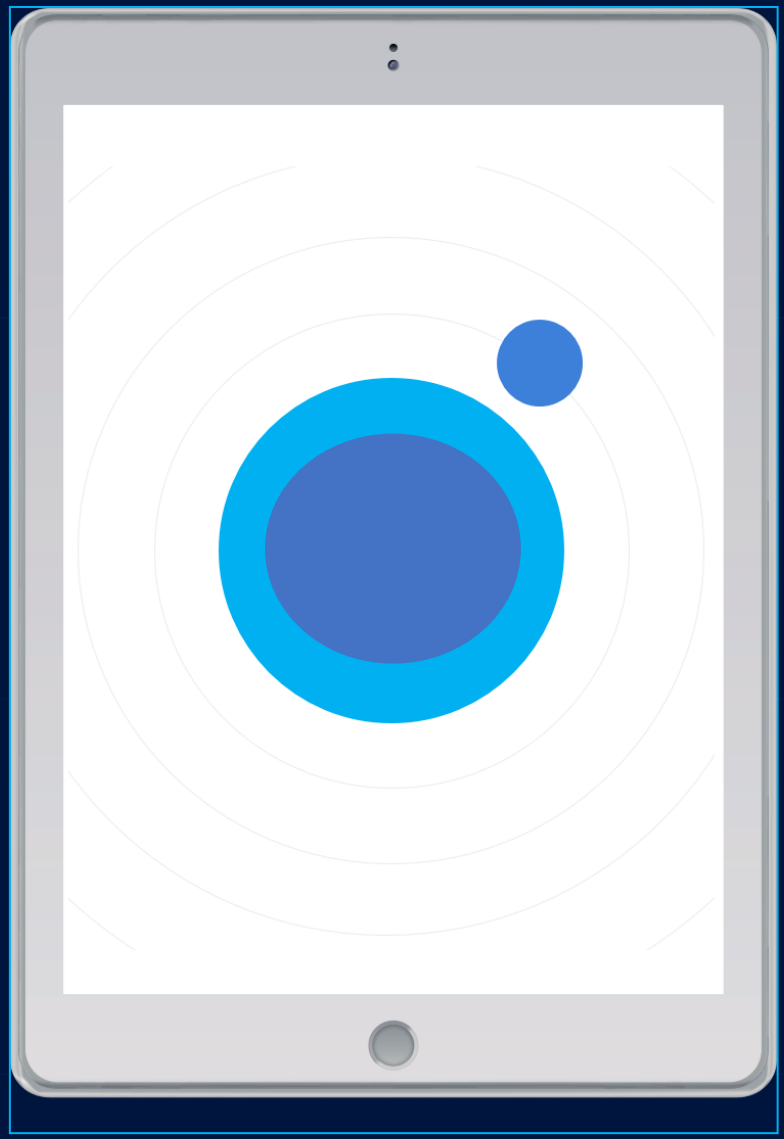
IT Security Officer

Name	
Title	
Signature	
Date	

Compliance Officer

Name	
Title	
Signature	
Date	

Account Request Form



3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.1[a] *authorized users are identified.*
	3.1.1[b] *processes acting on behalf of authorized users are identified.*
	3.1.1[c] *devices (and other systems) authorized to connect to the system are identified.*
	3.1.1[d] *system access is limited to authorized users.*
	3.1.1[e] *system access is limited to processes acting on behalf of authorized users.*
	3.1.1[f] *system access is limited to authorized devices (including other systems).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management].

Control Impact

Access Control	Identification and Authentication	System and Communications Protection	System and Information Integrity
3.1.1	3.5.1	3.13.3	3.14.7
3.1.2	3.5.2		
3.1.3	3.5.3		
3.1.4			
3.1.5			

Reading the Controls

NIST SP 800-171

1

Account Management Policy

2

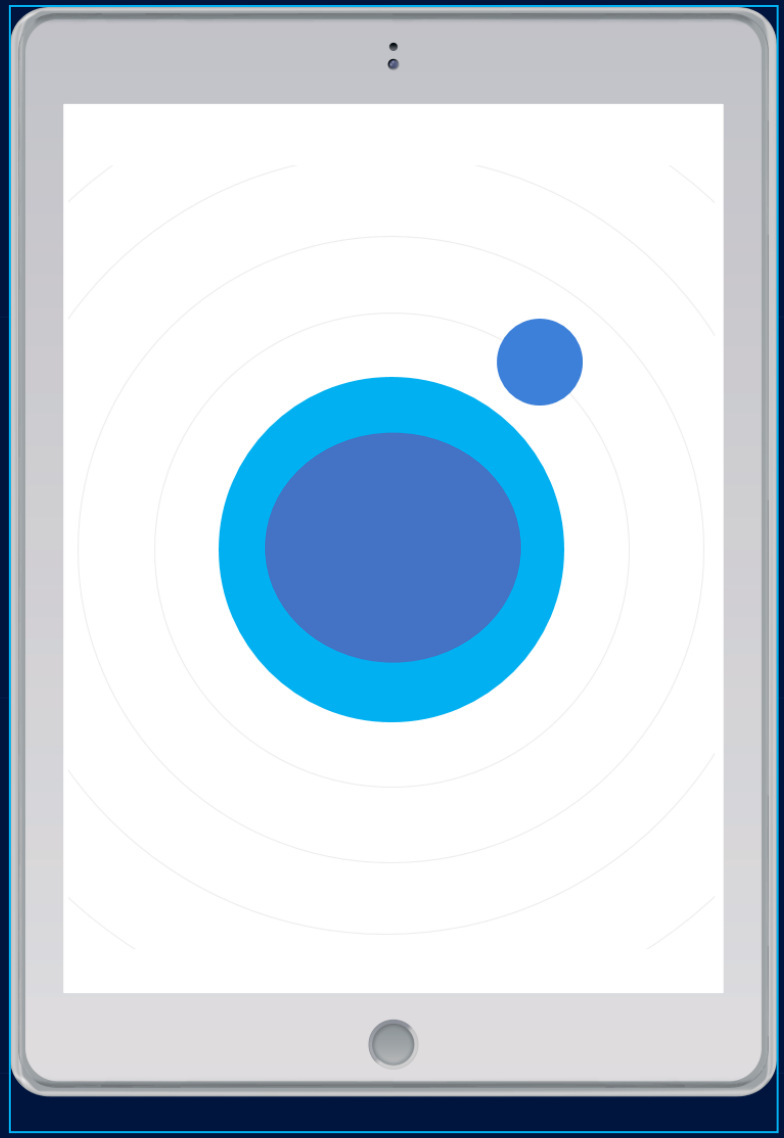
Acceptable Use Policy

3

Access Control Policy

TABLE OF CONTENTS

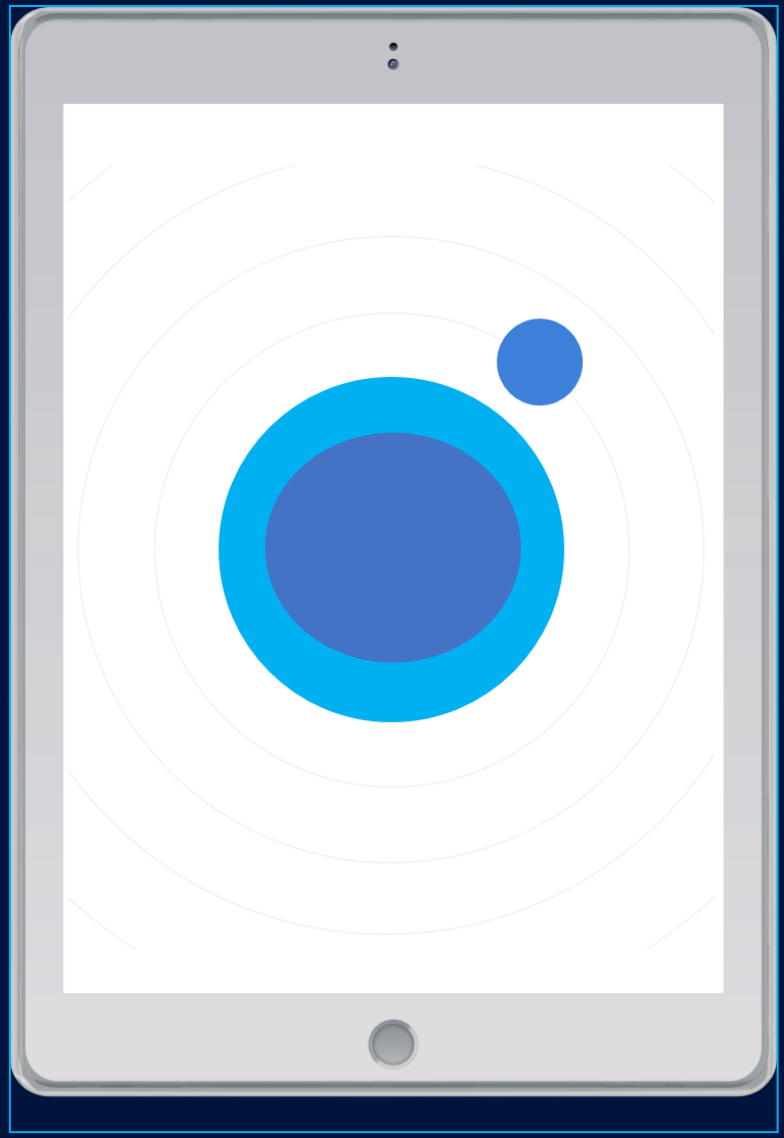
Acceptable Use Policy



Access Management

- Access to information is based on a "**need to know**".
- Personnel are permitted to use only those network and host addresses issued to them by [Company] IT and should not attempt to access any data or programs contained on [Company] systems for which they do not have authorization or explicit consent.
- All remote access connections made to internal [Company] networks and/or environments must be made through approved, and [Company]-provided, virtual private networks (VPNs).
- Personnel should not divulge any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their (personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),
    - Security Tokens (i.e. Smartcard),
    - Multi-factor authentication information
    - Access cards and/or keys,
    - Digital certificates,
    - Similar information or devices used for identification and authentication purposes.
- Access cards and/or keys that are no longer required must be returned to physical security personnel.
- Lost or stolen access cards, security tokens, and/or keys must be reported to physical security personnel as soon as possible.
- A service charge may be assessed for access cards, security tokens, and/or keys that are lost, stolen, or are not returned.

Acceptable Use Policy



Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following [Company] rules:
    - Must meet all requirements including minimum length, complexity, and reuse history.
    - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
    - Must not be the same passwords used for non-business purposes.
- Unique passwords should be used for each system, whenever possible.
- User account passwords must not be divulged to anyone. [Company] support personnel and/or contractors should never ask for user account passwords.
- If the security of a password is in doubt, the password should be changed immediately.
- Personnel should not circumvent password entry with application remembering, embedded scripts or hard coded passwords in client software.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with [Company], if issued.
- An approved User Account Request Form is required for any/all account creations.

Acceptable Use Policy

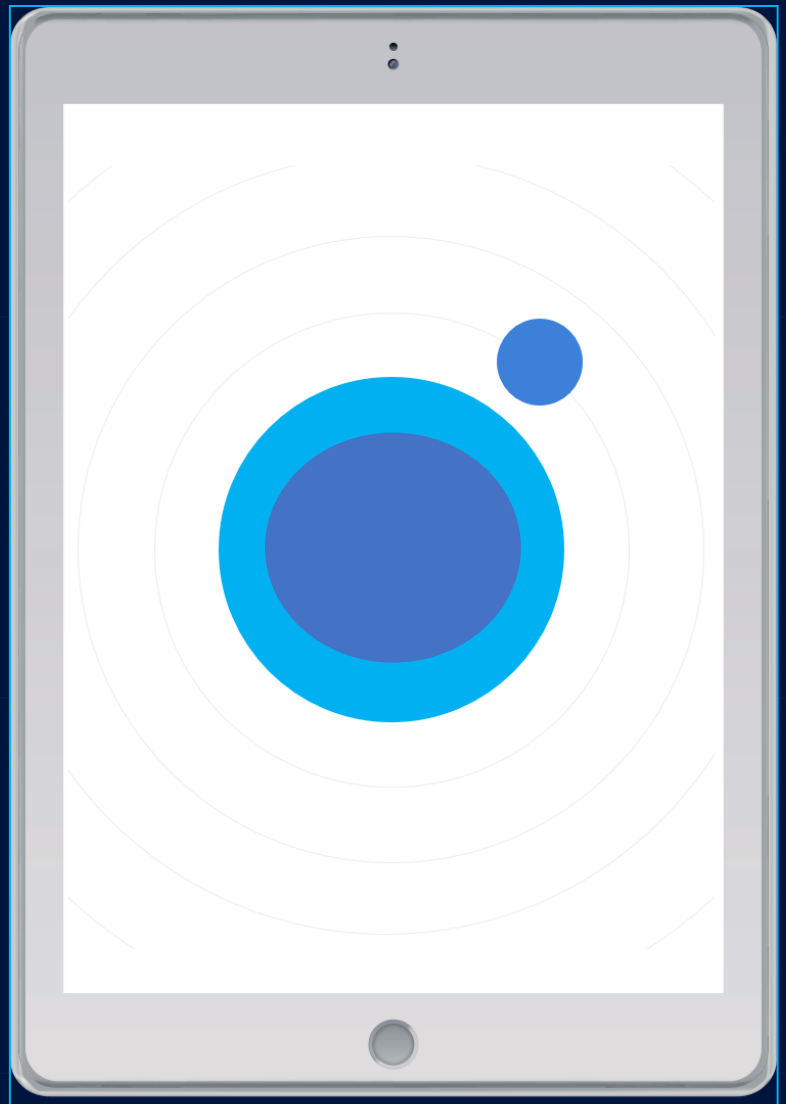
Acceptable Use Policy

3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.2[a]	*the types of transactions and functions that authorized users are permitted to execute are defined.*
	3.1.2[b]	*system access is limited to the defined types of transactions and functions for authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing access control policy].	

Acceptable Use

- Personnel are responsible for complying with [Company] policies when using [Company] information resources and/or on [Company] time. If requirements or responsibilities are unclear, please seek assistance from the Information Security Committee.
- Personnel are responsible for ensuring all corporate network/domain assets are used in accordance with all assigned job functions and responsibilities.
- Personnel must promptly report harmful events or policy violations involving [Company] assets or information to their manager or a member of the Incident Handling Team. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to [Company] **Information Resources**.
    - Data incident: any potential loss, theft, or compromise of [Company] information.
    - Unauthorized access incident: any potential unauthorized access to a [Company] **Information Resource**.
    - Facility security incident: any damage or potentially unauthorized access to a [Company] owned, leased, or managed facility.
    - Policy violation: any potential violation to this or other [Company] policies, standards, or procedures.
- Personnel should not purposely engage in activity that may
    - harass, threaten, impersonate, or abuse others;
    - degrade the performance of [Company] **Information Resources;**
    - deprive authorized [Company] personnel access to a [Company] **Information Resource;**

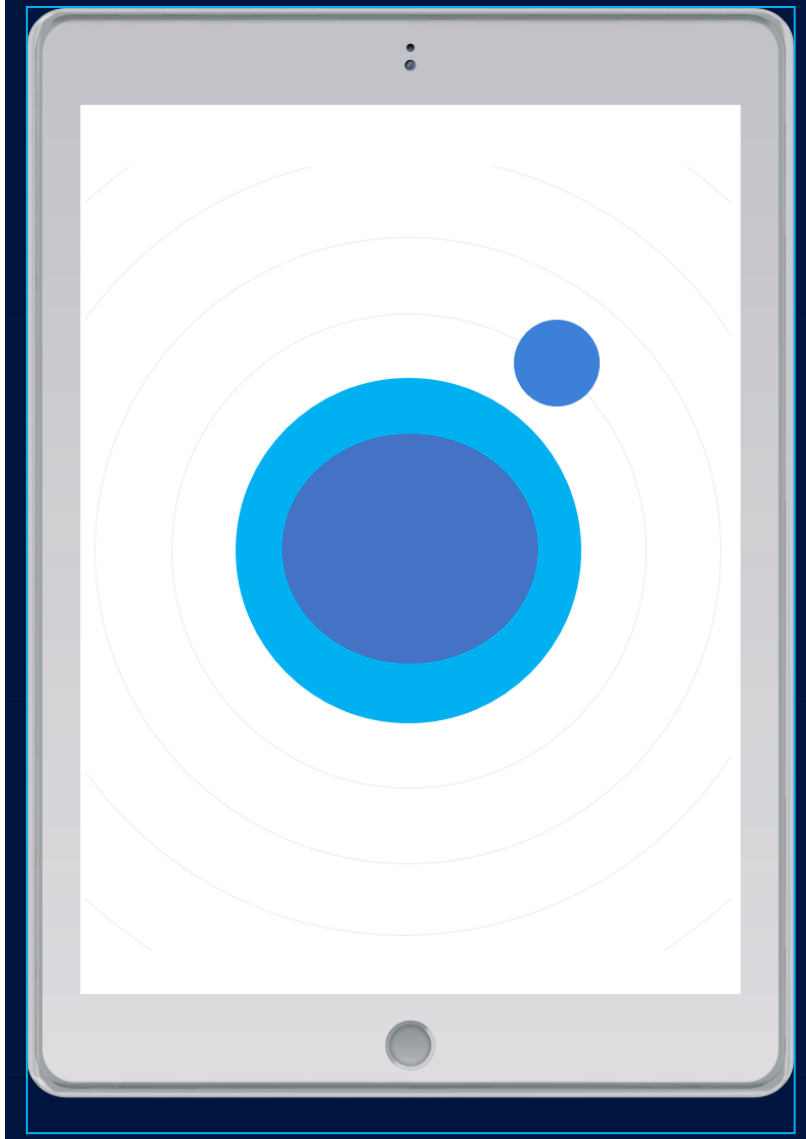
Acceptable Use Policy



- obtain additional resources beyond those allocated;
- or circumvent [Company] computer security measures.

- Personnel should not download, install, or run security programs or utilities that reveal or exploit weakness in the security of a system. For example, [Company] personnel should not run password cracking programs, packet sniffers, port scanners, or any other non-approved programs on any [Company] **Information Resource**.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed on [Company] time and/or using [Company] **Information Resources** are the property of [Company].
- Use of encryption should be managed in a manner that allows designated [Company] personnel to promptly access all data.
- [Company] **Information Resources** are provided to facilitate company business and should not be used for personal financial gain.
- Personnel are expected to cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to respect and comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using [Company] **Information Resources**.
- Personnel should not intentionally access, create, store or transmit material which [Company] may deem to be offensive, indecent, or obscene.

Acceptable Use Policy



Acceptable Use Policy

3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.2[a]	*the types of transactions and functions that authorized users are permitted to execute are defined.*
	3.1.2[b]	*system access is limited to the defined types of transactions and functions for authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing access control policy].	

Reading the Controls

NIST SP 800-171

1

Account Management Policy

2

Acceptable Use Policy

3

Access Control Policy

Permissions

3.1.5	**SECURITY REQUIREMENT** Employ the principle of least privilege, including for specific security functions and privileged accounts.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.5[a] *privileged accounts are identified.*
	3.1.5[b] *access to privileged accounts is authorized in accordance with the principle of least privilege.*
	3.1.5[c] *security functions are identified.*
	3.1.5[d] *access to security functions is authorized in accordance with the principle of least privilege.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; list of conditions for group and role membership; notifications or records of recently transferred, separated, or terminated employees; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring/audit records; procedures addressing least privilege; list of security functions (deployed in hardware, software, and firmware) and security-relevant information for which access is to be explicitly authorized; list of system-generated privileged accounts; list of system administration personnel; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities; personnel with responsibilities for defining least privileges necessary to accomplish specified tasks]. Test: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management; mechanisms implementing least privilege functions; mechanisms prohibiting privileged access to the system].

Access Control Principles

3.1 Least Privilege

The principle of least privilege dictates that users are granted the minimum level of access necessary to perform their job functions. This approach reduces the risk of unauthorized access and limits the potential damage from security breaches. Key aspects include:

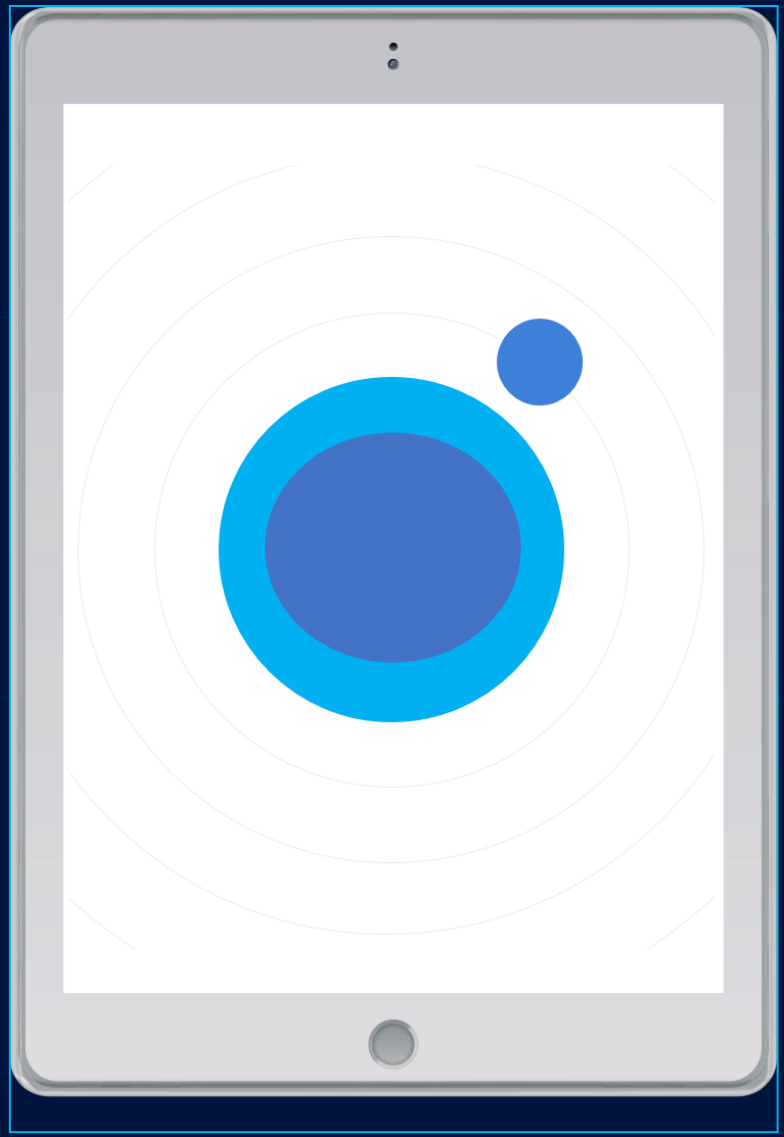
- **Access Limitation**: Users should only have access to information and systems that are essential for their roles.
- **Regular Reviews**: Periodic reviews of access rights to ensure that they remain appropriate as job responsibilities change.
- **Access Adjustment**: Prompt adjustment of access rights when users change roles or leave the organization.

3.2 Need to Know

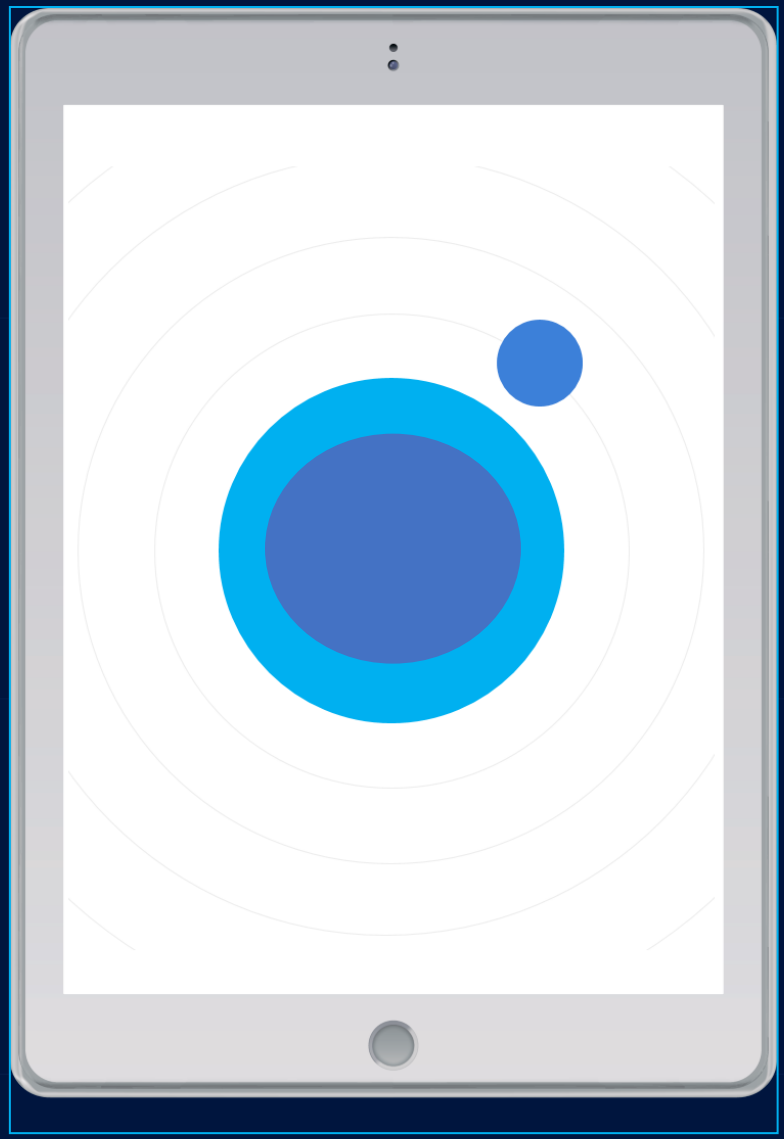
Access to CUI and other sensitive information is granted based on a clear business need to know. Users must demonstrate a legitimate need for access to specific information to fulfill their job duties. Key aspects include:

- **Justification**: Access requests must include a valid business justification.
- **Approval**: Requests for access to sensitive information require approval from relevant authorities, such as data owners and security officers.

Access Control Policy



Access Control Policy



3.3 Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is used to manage access rights based on user roles within the organization. Each role is associated with specific access permissions that reflect job responsibilities and security requirements. Key aspects include:

- **Role Definition**: Clearly defined roles with associated access permissions.
- **Role Assignment**: Users are assigned roles based on their job functions.
- **Role Reviews**: Regular reviews of roles and associated permissions to ensure they remain aligned with organizational needs and security policies.

Pulling It All Together

- User Identification and Authentication
- Access Request and Approval
- Access Provisioning
- Access Monitoring
- Access Revocation

Access Management

4.1 User Identification and Authentication

All users must be uniquely identified and authenticated before accessing organizational resources. Robust identification and authentication mechanisms are critical for ensuring that only authorized individuals gain access. Key aspects include:

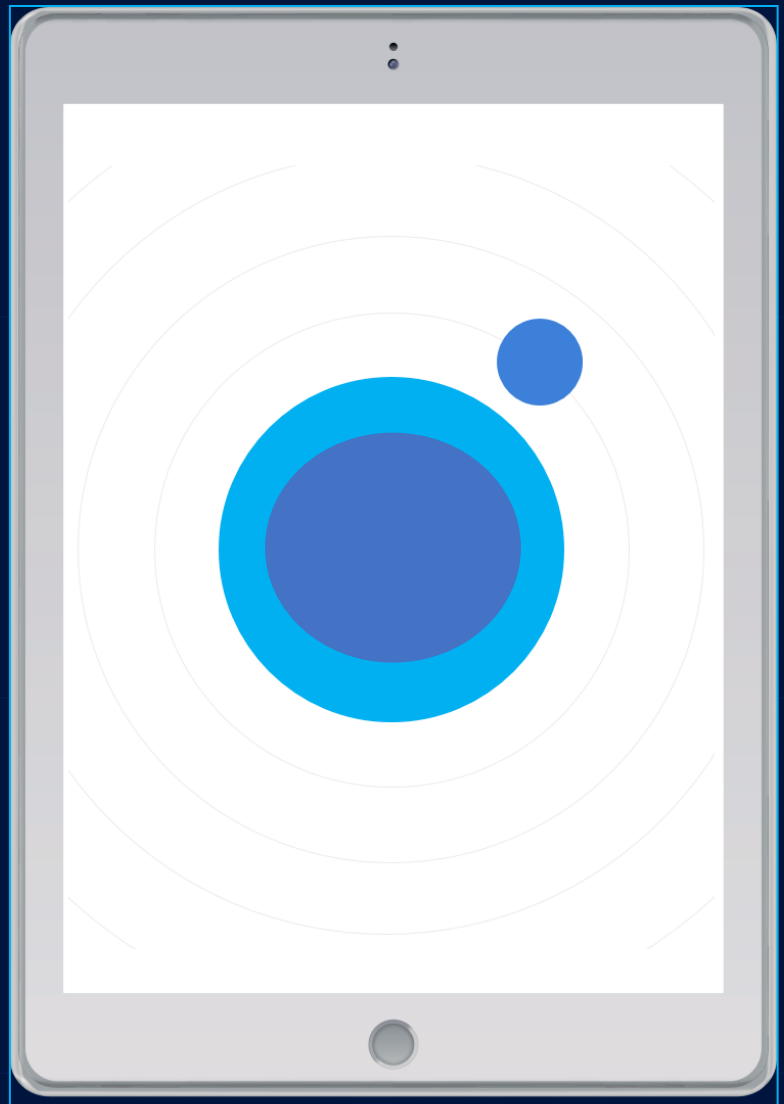
- **User IDs**: Unique user IDs are assigned to each user to ensure individual accountability. User IDs must not be shared or reused.
- **Passwords**: Strong password policies are enforced, requiring complex passwords that are changed regularly. Passwords must meet the organization's complexity requirements and must not be reused across different accounts.
- **Multi-Factor Authentication (MFA)**: MFA is required for accessing sensitive systems and data. This adds an additional layer of security by requiring users to provide two or more verification factors to gain access.

4.2 Access Request and Approval

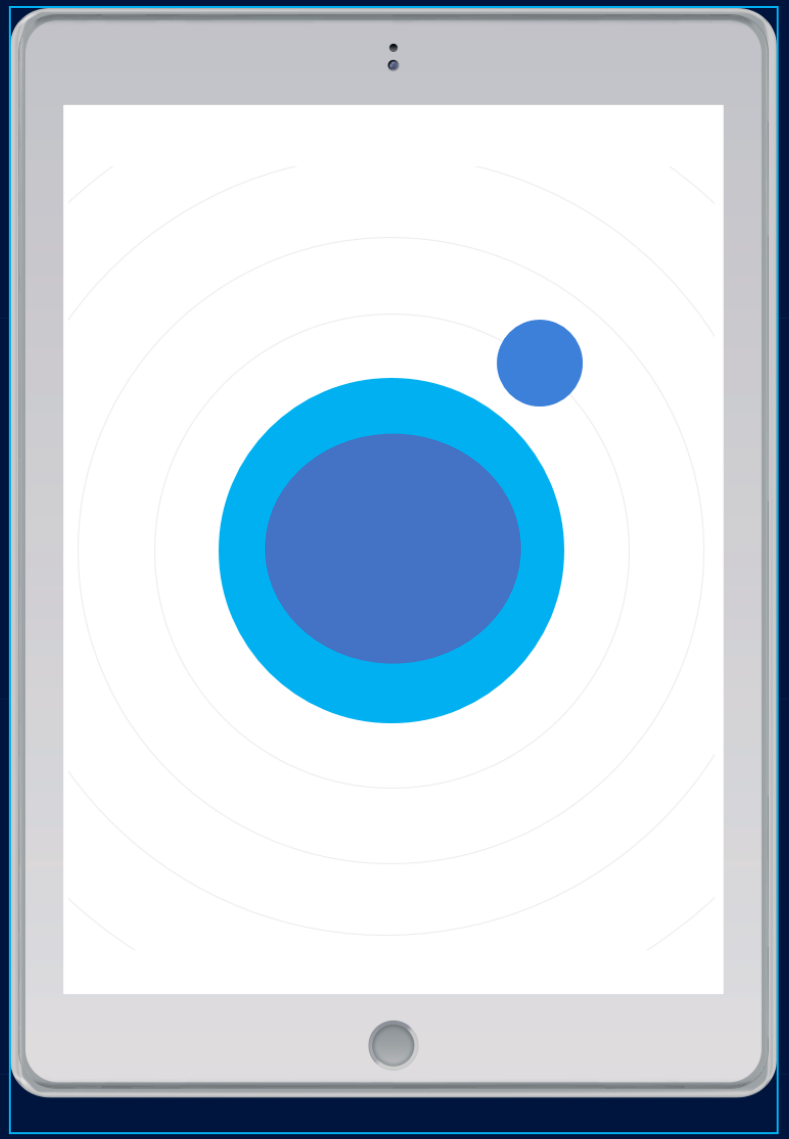
Access to information systems and data must be formally requested and approved through a defined process. This ensures that access is granted based on legitimate needs and appropriate authorization. Key aspects include:

- **Access Request Form**: Users must complete an Access Request Form, detailing the resources they need access to and the justification for access. The form must be submitted to the relevant authorities for approval.
- **Approval Workflow**: Access requests must follow a predefined approval workflow. Requests must be reviewed and approved by the user's immediate supervisor, the IT Security Officer, and, if applicable, the data owner. Approval must be documented and retained for audit purposes.

Access Control Policy



Access Control Policy



4.3 Access Provisioning

Once approved, access is provisioned according to established procedures to ensure that users receive the appropriate access rights. Key aspects include:

- **User Account Creation**: IT personnel create user accounts with the appropriate access rights based on the approved request.
- **Role Assignment**: Users are assigned to roles that correspond to their job responsibilities and approved access levels.
- **Access Reviews**: Regular reviews of user access rights are conducted to ensure they remain appropriate for the user's role and responsibilities. Any discrepancies are addressed promptly.

4.4 Access Modification

Access rights must be modified promptly when there are changes in user roles, responsibilities, or employment status. This ensures that access remains aligned with current job functions and security requirements. Key aspects include:

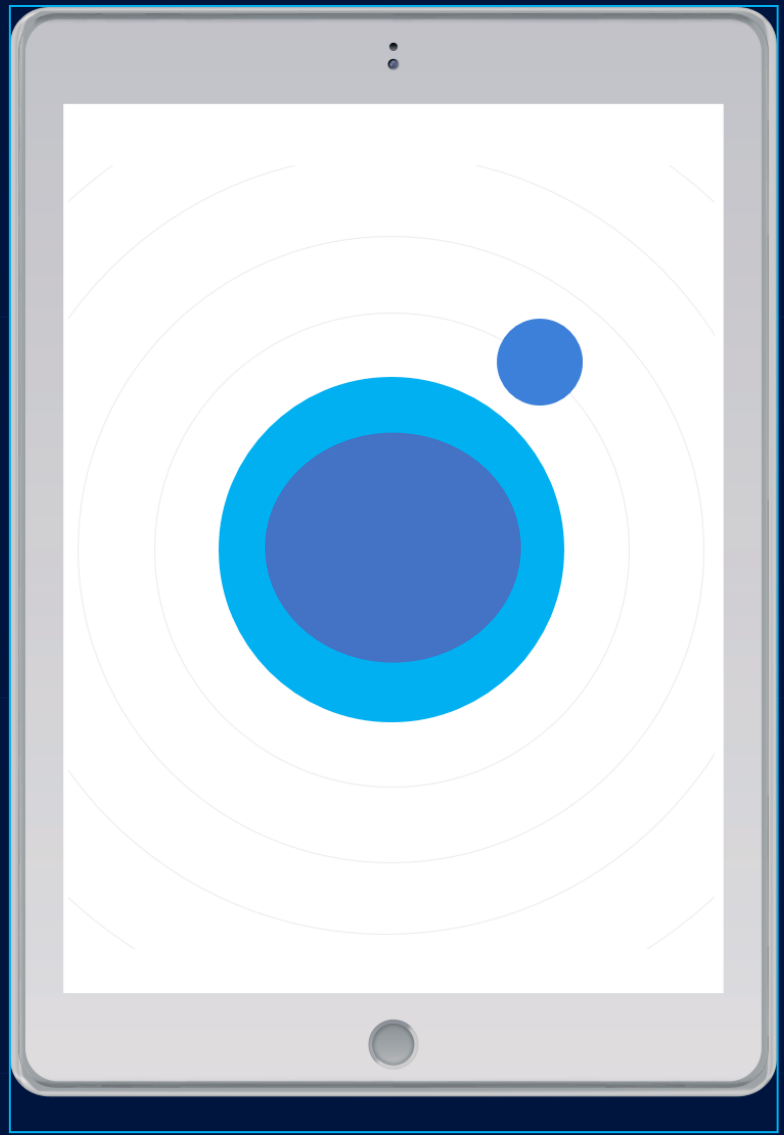
- **Modification Request**: Users or their supervisors must submit a request to modify access rights when there are changes in roles or responsibilities. The request must include a justification for the change.
- **Approval and Implementation**: Modification requests must follow the same approval workflow as access requests. Approved changes are implemented promptly by IT personnel, and the modifications are documented.

4.5 Access Revocation

Access rights must be revoked promptly when users no longer require access, such as upon termination or role change. This minimizes the risk of unauthorized access by former employees or individuals whose job functions no longer require certain access rights. Key aspects include:

- **Termination of Access**: IT personnel must promptly disable user accounts and revoke access rights upon termination or role change. This includes deactivating accounts, removing access to systems and data, and reclaiming organizational assets.
- **Exit Interviews**: Exit interviews are conducted to ensure all organizational resources are returned, and access rights are revoked. Users are reminded of their ongoing obligations regarding confidentiality and the handling of organizational information.

Access Control Policy

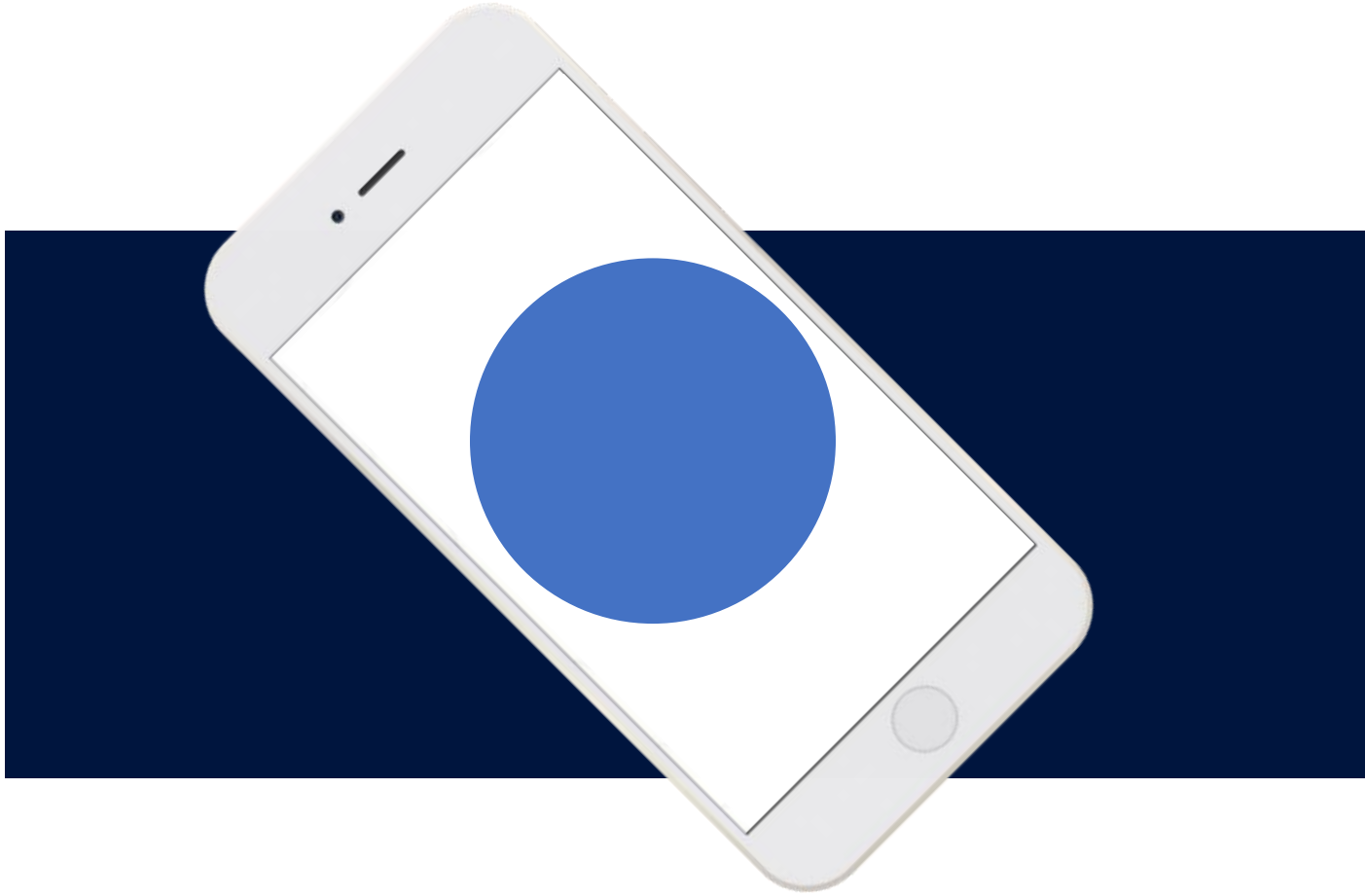


Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

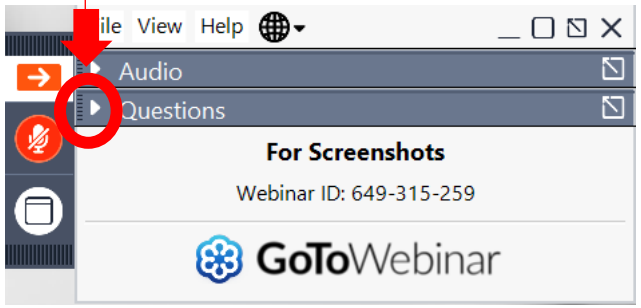
AN APEX ACCELERATOR



QUESTIONS?

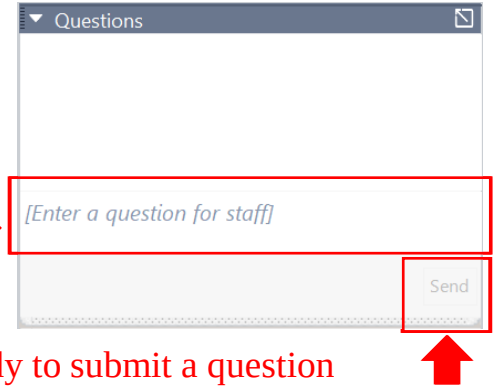
OPENING THE QUESTIONS BOX

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

CYBER FRIDAY LIVE WEBINAR SERIES

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **May 17,** 3.1.1 Access Control Lists, Account Request Documentation, and Acceptable User Policies
- **June 21,** 3.1.2 Security Awareness Training, Role-Based Training, and Insider Threat Training
- **July 19,** 3.1.3 Audit and Accountability Policy, Log Review Procedure
- **August 23,** 3.1.4 Configuration Management Policy, Change Request Process, Baseline Configurations
- **September 20,** 3.1.6 Incident Response Policy, Incident Response Plan
- **October 18,** 3.1.7 System Maintenance Policy
- **November 22,** 3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security
- **January 24,** 3.1.11 Risk Assessment Policy, Security Assessment Reports

WPI Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

18th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In Partnership with Wisconsin's Military Installations

June 10

Fort McCoy

June 20

Volk Field ANGB

GOBC will provide you the opportunity to gain insights into:

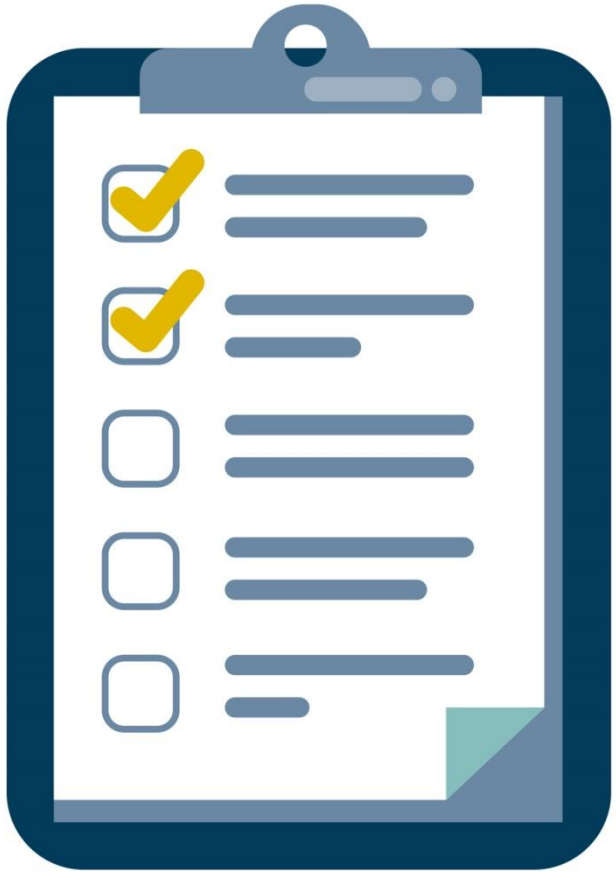
- *COFFEE with the COMMANDER*
- Current operations and priorities at Wisconsin's Federal and State government agencies and military facilities
- Connecting with agency and installation leadership, operational staff and buyers
- Locating and bidding on current and future procurement opportunities
- Resources available to assist your business in winning government prime and subcontracts

…More information and registrations at wispro.org/events

WPI Wisconsin Procurement Institute
An APEX Accelerator

NCMA National Contract Management Association
WISCONSIN

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

May 15, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

CONTINUING PROFESSIONAL EDUCATION

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

Neelu Patil
neelagangap@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MattF@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226