Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:

Building a CMMC Model: 3.1.7 System Maintenance Policy

October 18| 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

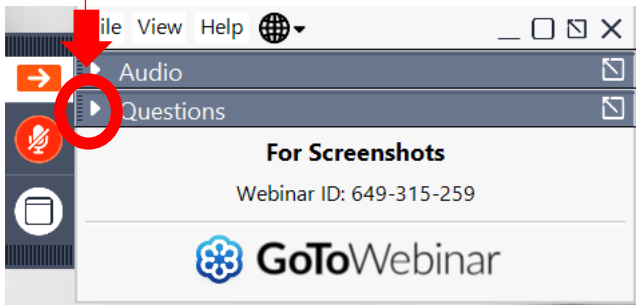
PLEASE

- 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!

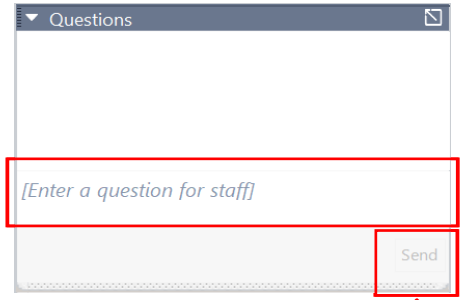
OPENING THE QUESTIONS BOX

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.

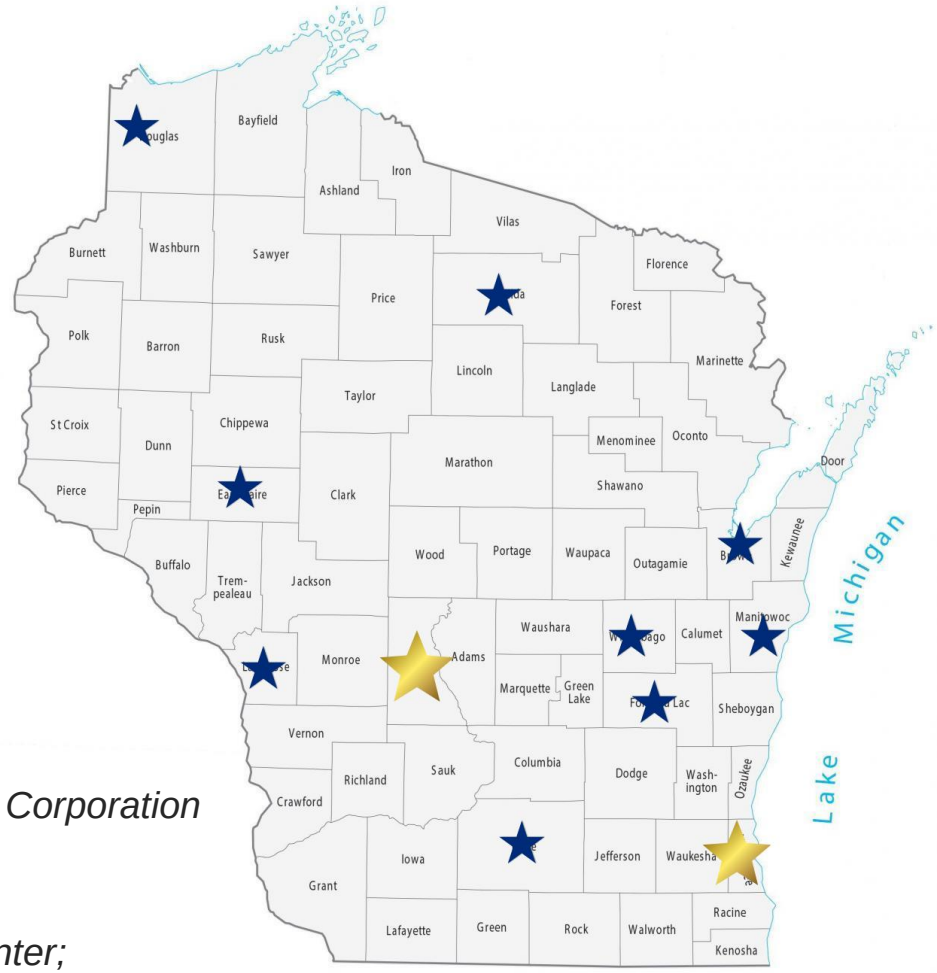
WPI provides services to all of Wisconsin's 72 counties

- 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……

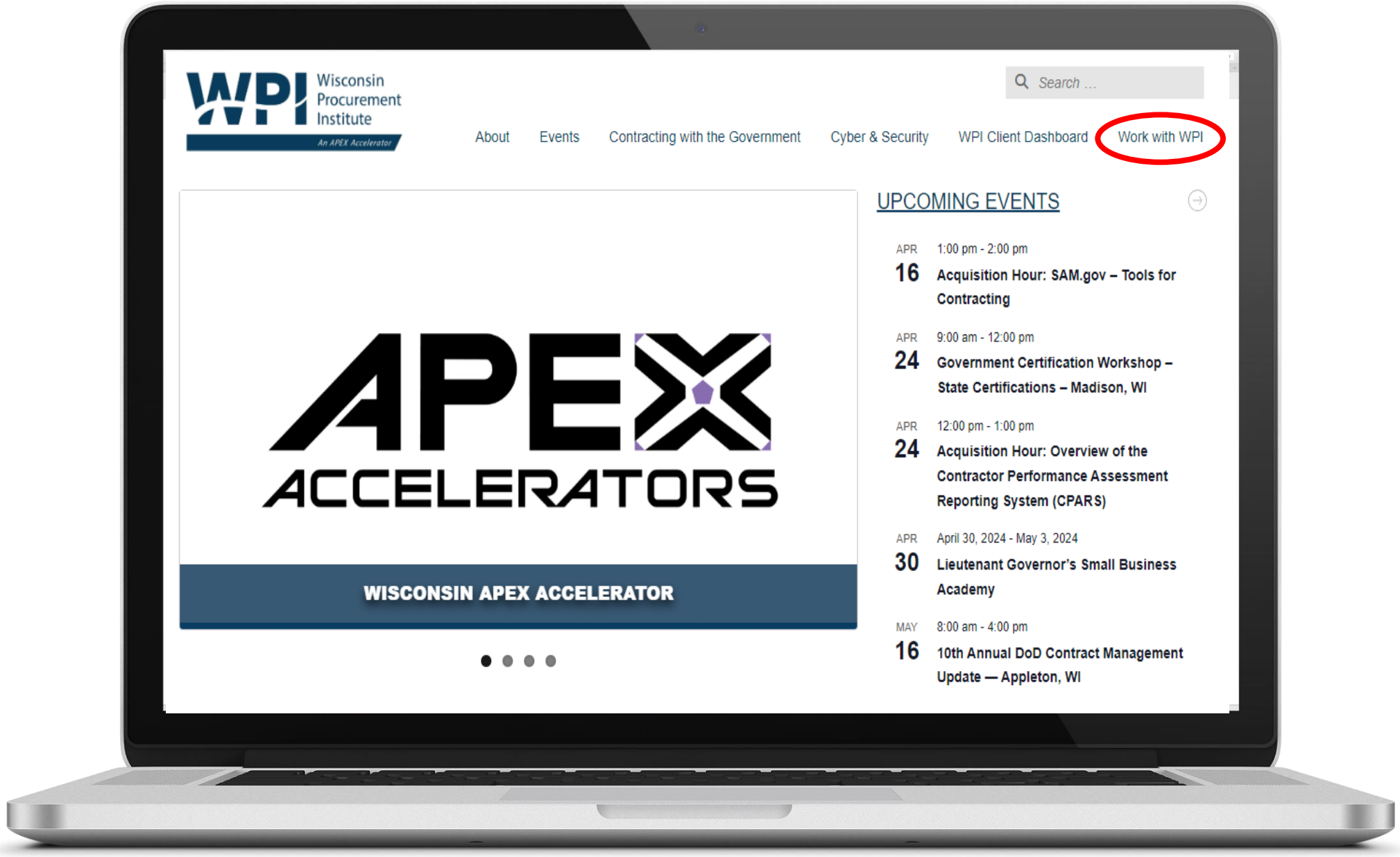
www.wispro.org

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*



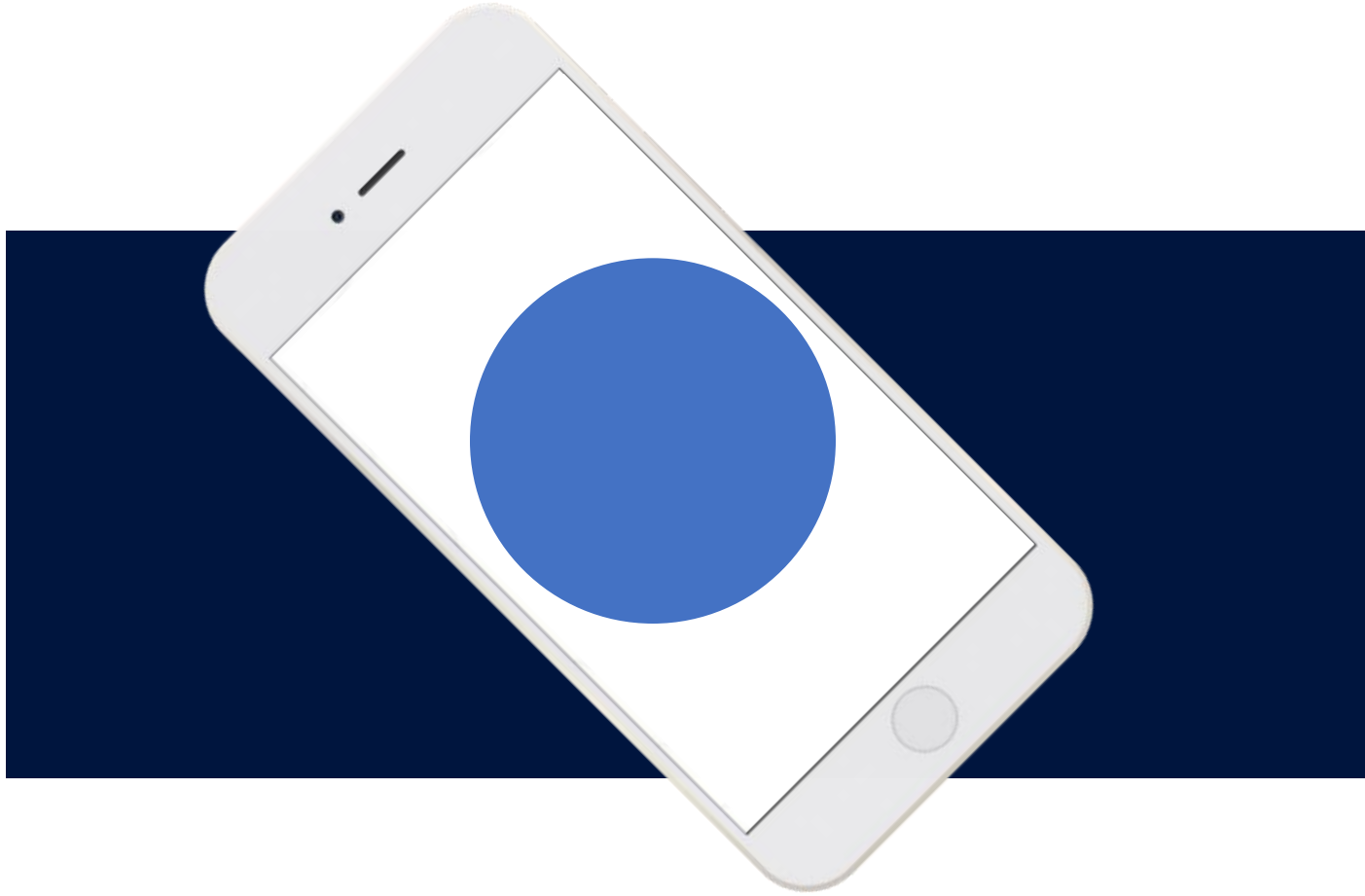
Wisconsin Procurement Institute
An APEX Accelerator


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 – October 18th, 2024

DFARS 252.204-7012

NIST
National Institute of Standards and Technology

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

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.

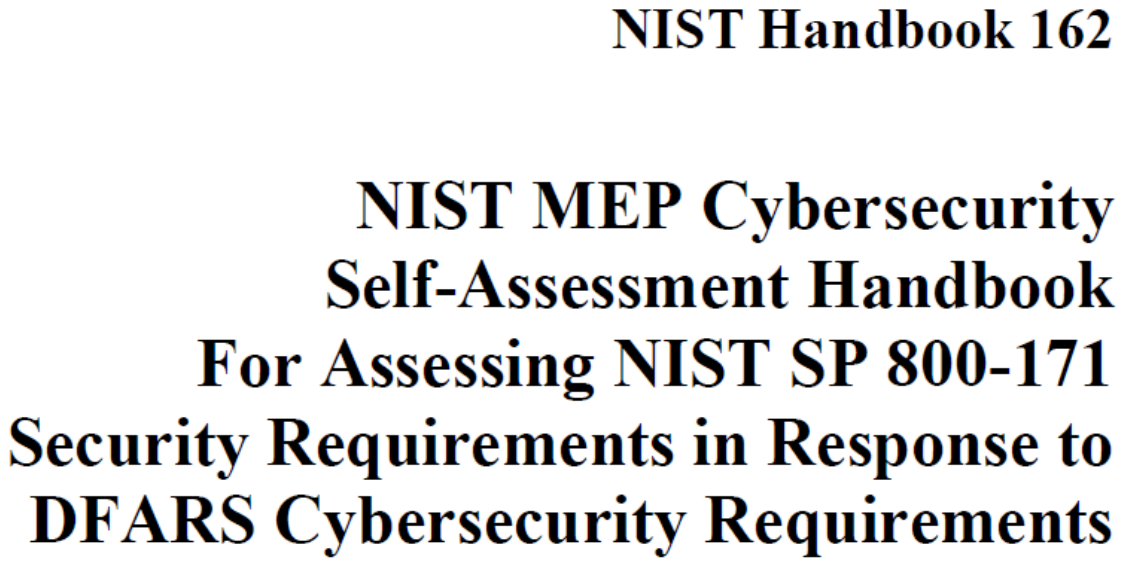
DFARS 252.204-7021

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 & 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

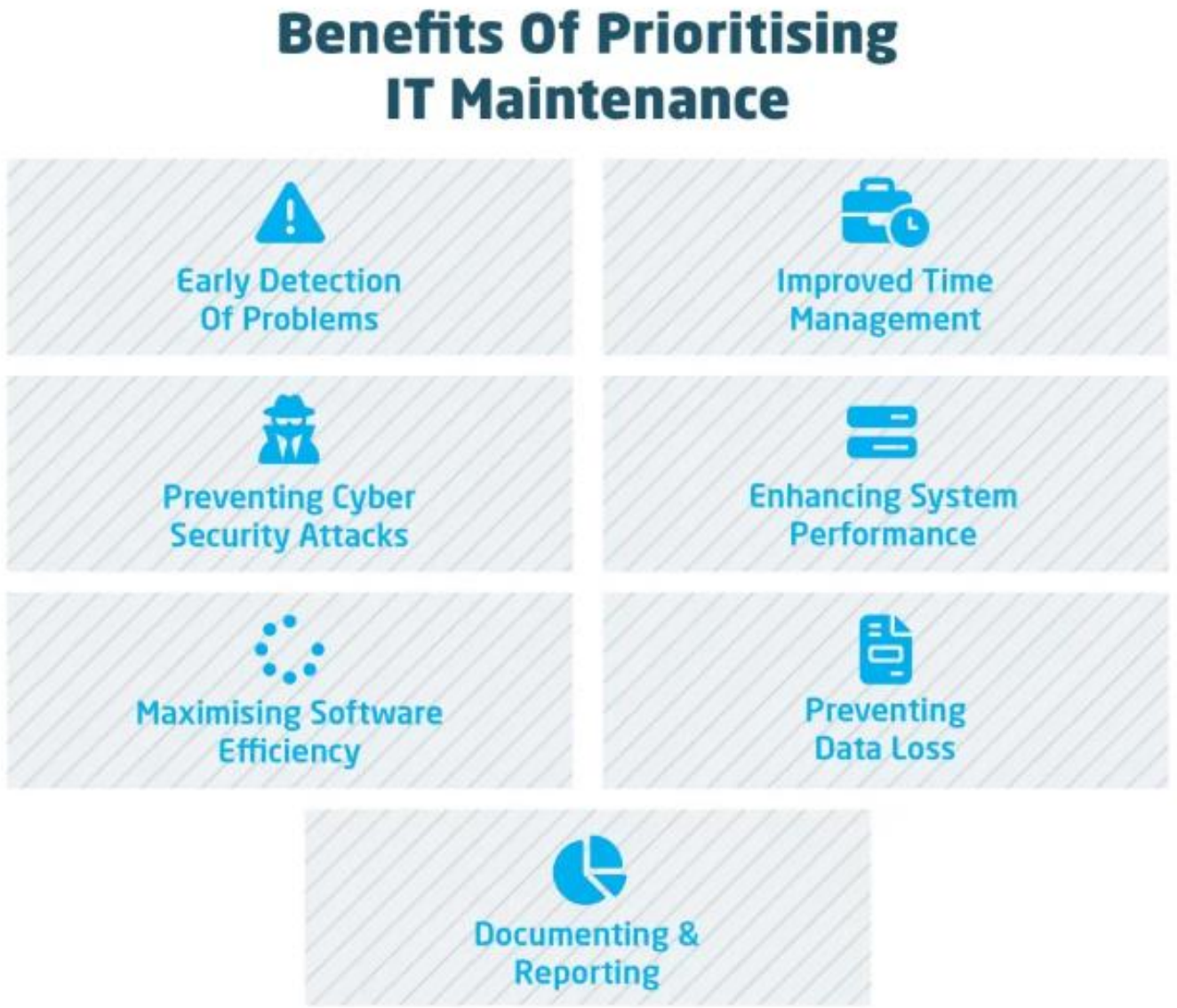
2 NIST SP 800-171A

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

3 NIST SP 800-18r1

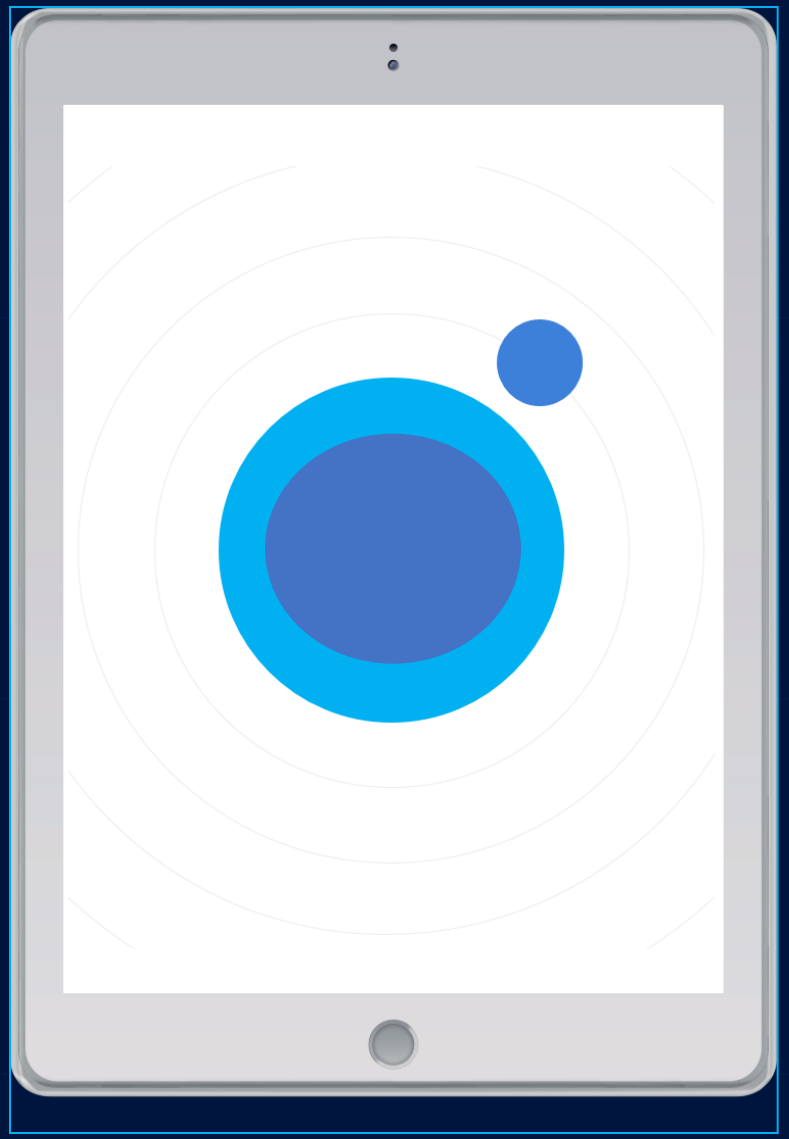
NIST Special Publication 800-18
Revision 1
Guide for Developing Security Plans for Federal Information Systems

Maintenance



Elements of the Policy

1. Purpose
2. Scope
3. Policy Statement
4. Definitions
    1. Maintenance Goals and Purpose
    2. Procedures
    3. Tools
5. Roles and Responsibilities
    - System Owner
    - IT Manager/Administrator
    - IT Maintenance Personnel
    - Security Officer
    - 3rd Party Providers/Vendors



Incident Response Team

Information Owner

- ❑ Ownership and Authority
- ❑ Leadership and Delegation
- ❑ Accountability

IT Manager/Leader

- ❑ Technical Response
- ❑ Translating Concerns and Solutions
- ❑ Dictating Expectations
- ❑ Security Oversight

IT Maintenance Personnel

- ❑ Executing Maintenance
- ❑ Documenting Process Completion
- ❑ Review Processes and Ensure Compliance

3rd Party Providers

- ❑ Support as dictated by SLA
- ❑ Communicate Clearly with

3.7.1	**SECURITY REQUIREMENT** Perform maintenance on organizational systems.
	ASSESSMENT OBJECTIVE *Determine if system maintenance is performed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System maintenance policy; procedures addressing controlled system maintenance; maintenance records; manufacturer or vendor maintenance specifications; equipment sanitization records; media sanitization records; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities; personnel responsible for media sanitization; system or network administrators]. Test: [*SELECT FROM:* Organizational processes for scheduling, performing, documenting, reviewing, approving, and monitoring maintenance and repairs for systems; organizational processes for sanitizing system components; mechanisms supporting or implementing controlled maintenance; mechanisms implementing sanitization of system components].

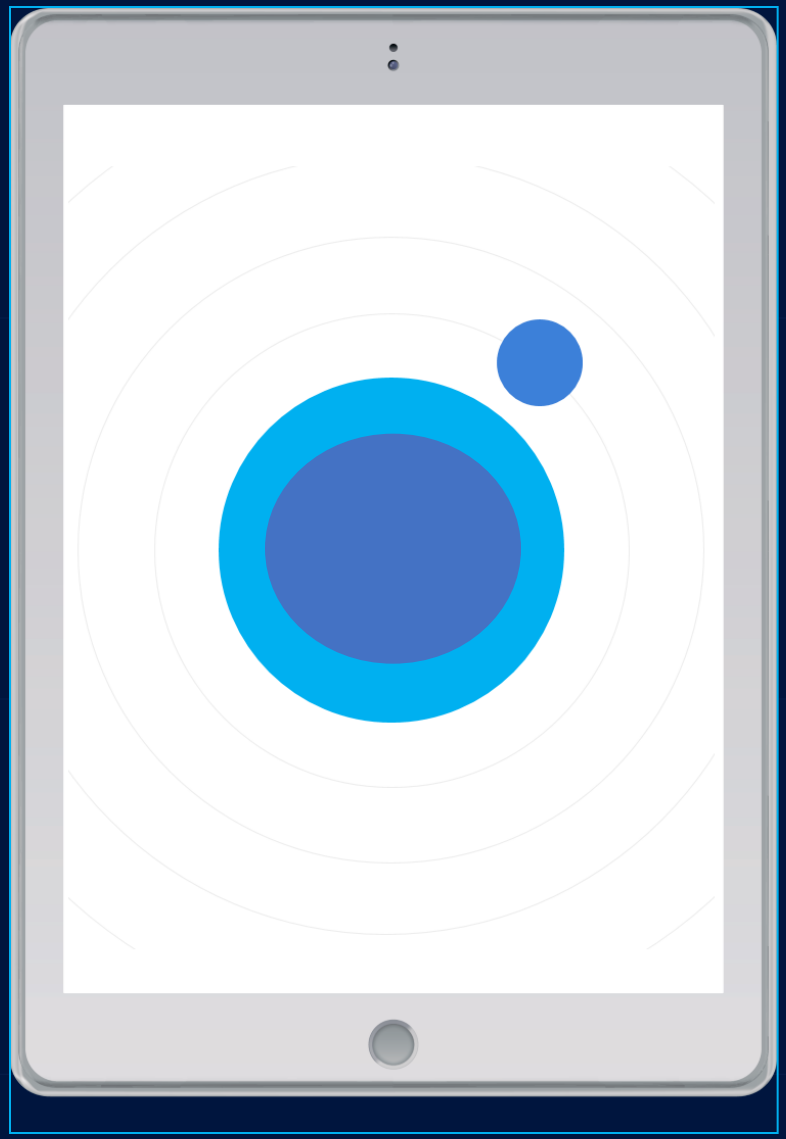
Elements of the Policy

3. Policy Statements

3.1 Authorized Personnel for Maintenance (3.7.1)

•Only qualified and authorized personnel are allowed to perform maintenance on organizational systems.

- **Internal Maintenance Personnel**: All staff must be authorized by the system owner and have completed appropriate training before performing maintenance tasks.
- **Third-Party Vendors**: External maintenance personnel must be vetted, and service agreements must include clauses that enforce compliance with security policies.
- **Documentation Requirement**: Records must be maintained for each maintenance activity, including the personnel involved, date, time, and system details.



3.7.2	**SECURITY REQUIREMENT** Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

ASSESSMENT OBJECTIVE

Determine if:

3.7.2[a]	*tools used to conduct system maintenance are controlled.*
3.7.2[b]	*techniques used to conduct system maintenance are controlled.*
3.7.2[c]	*mechanisms used to conduct system maintenance are controlled.*
3.7.2[d]	*personnel used to conduct system maintenance are controlled.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools and media; maintenance records; system maintenance tools and associated documentation; maintenance tool inspection records; system security plan; other relevant documents or records].

Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities].

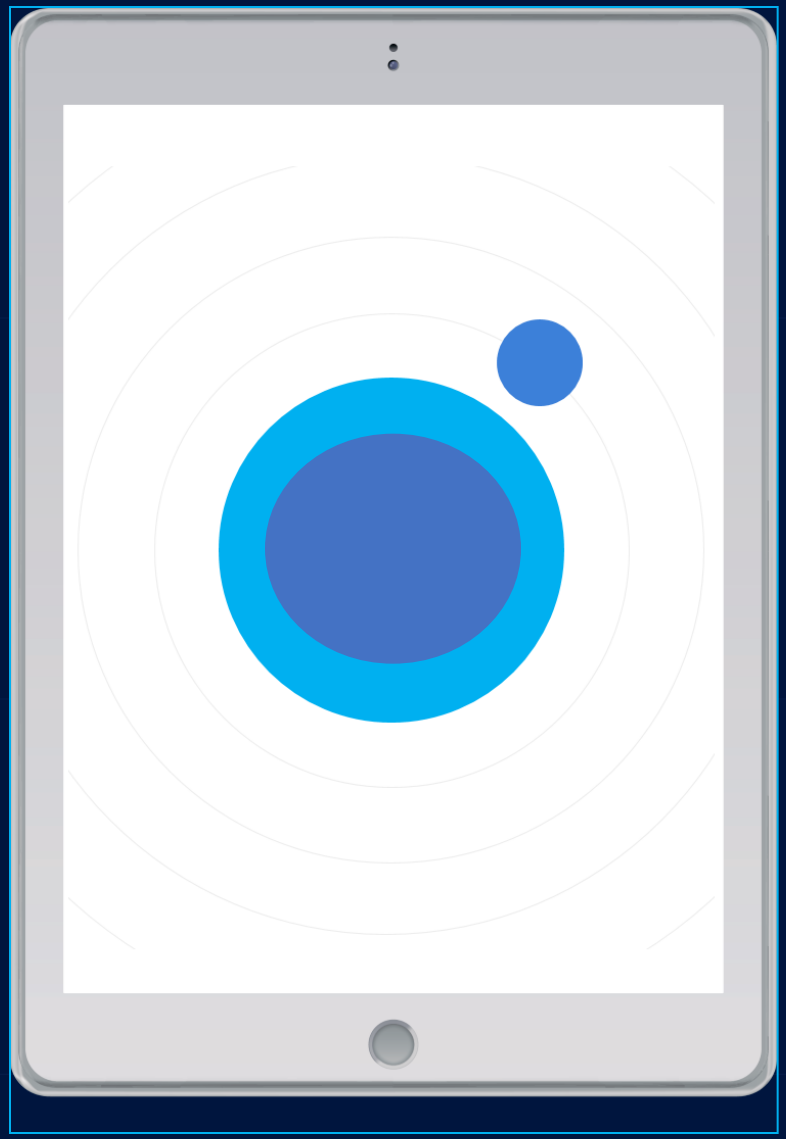
Test: [*SELECT FROM:* Organizational processes for approving, controlling, and monitoring maintenance tools; mechanisms supporting or implementing approval, control, and monitoring of maintenance tools; organizational processes for inspecting maintenance tools; mechanisms supporting or implementing inspection of maintenance tools; organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

3.2 Maintenance Tools (3.7.2)

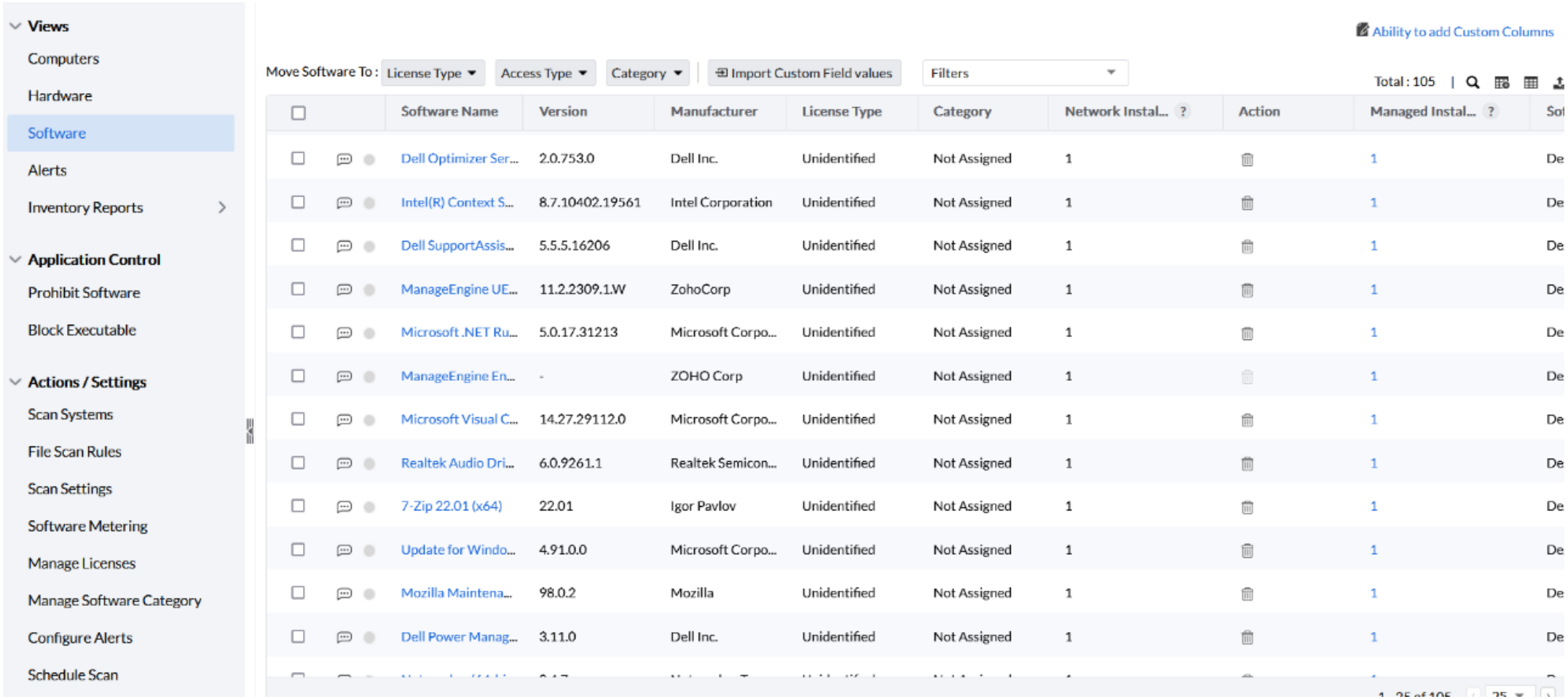
•All tools used for maintenance must be controlled and approved.

- **Secure Tools**: Maintenance tools (hardware or software) must be validated and secured before use to prevent the introduction of malicious code or vulnerabilities.
- **Tool Inventory**: A list of approved tools will be maintained, and only these tools may be used during maintenance activities.
- **Tool Access Controls**: Access to maintenance tools must be restricted to authorized personnel only.
- **Documentation Requirement**: A log must be kept detailing the tools used for each maintenance task.

Elements of the Policy



IT Tool Inventory



3.7.4	**SECURITY REQUIREMENT** Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
	ASSESSMENT OBJECTIVE *Determine if media containing diagnostic and test programs are checked for malicious code before being used in organizational systems that process, store, or transmit CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System maintenance policy; procedures addressing system maintenance tools; system maintenance tools and associated documentation; maintenance records; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational process for inspecting media for malicious code; mechanisms supporting or implementing inspection of media used for maintenance].

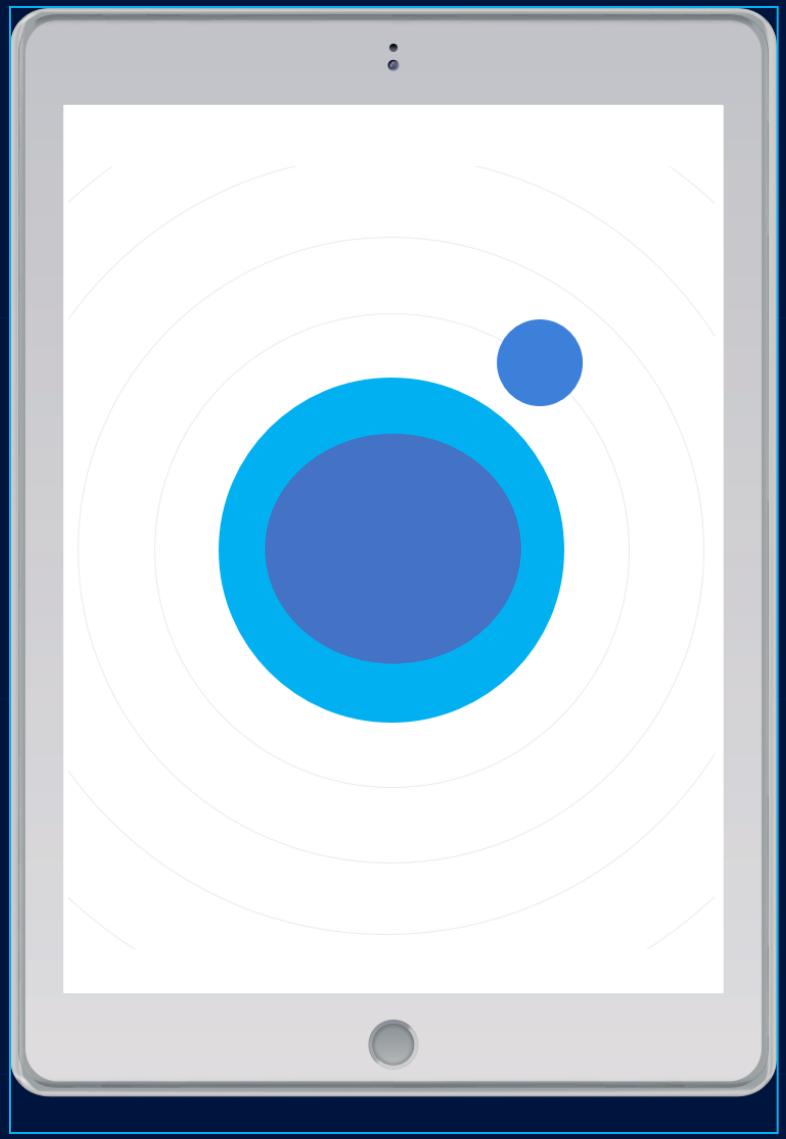
3.7.5	**SECURITY REQUIREMENT** Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.7.5[a]	*multifactor authentication is used to establish nonlocal maintenance sessions via external network connections.*
	3.7.5[b]	*nonlocal maintenance sessions established via external network connections are terminated when nonlocal maintenance is complete.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System maintenance policy; procedures addressing nonlocal system maintenance; system security plan; system design documentation; system configuration	

Elements of the Policy

3.3 Remote Maintenance (3.7.3)

•**Remote Maintenance**: Remote maintenance must be performed securely and authorized in advance.

- **Encryption**: Remote maintenance sessions must use encrypted communication channels (e.g., VPN or secure SSH).
- **Multi-Factor Authentication (MFA)**: Remote access for maintenance activities requires MFA to authenticate users.
- **Monitoring**: All remote maintenance activities must be monitored and logged in real time to ensure security controls are maintained.
- **Approval Process**: Remote maintenance must be pre-approved by the system owner, with specific authorization for each session.
- **Documentation Requirement**: Logs must include the time and duration of remote access, personnel involved, tools used, and system changes made.

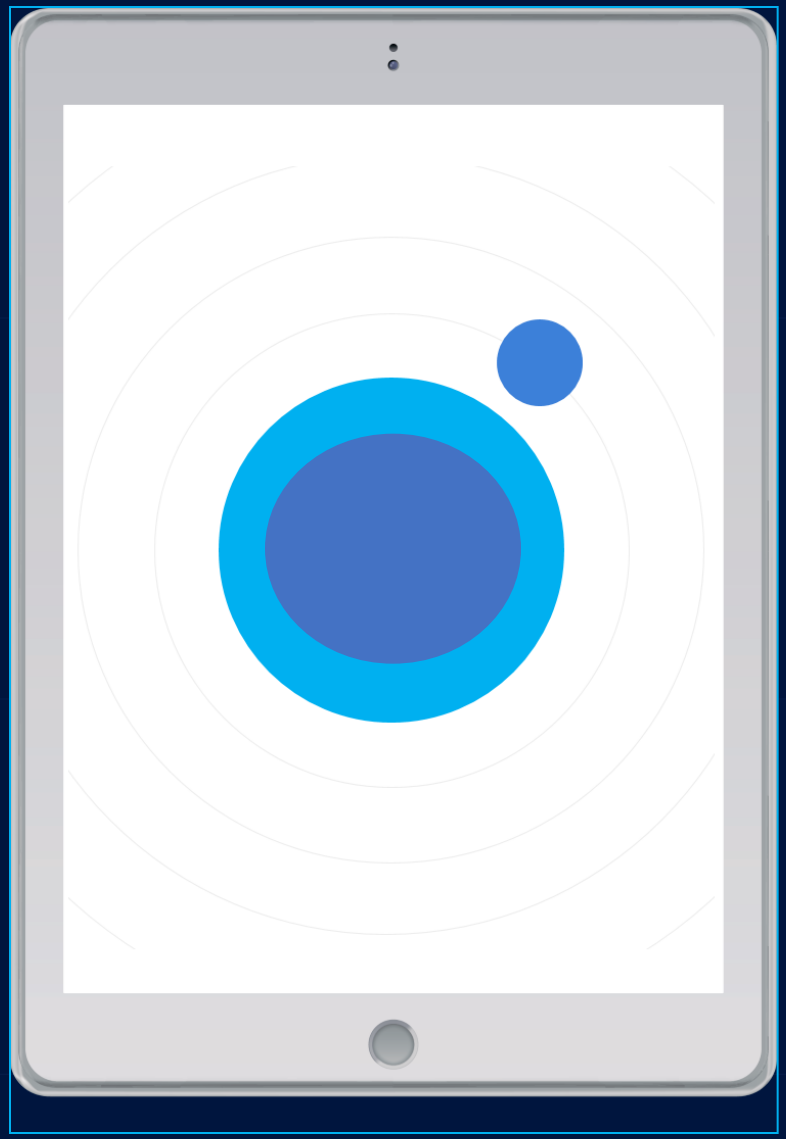


Elements of the Policy

3.4 Non-Local Maintenance (3.7.4)

•Maintenance conducted by third-party vendors or personnel not physically on-site must follow strict security protocols.

- **Vendor Agreements**: All third-party vendors must sign agreements that include security requirements consistent with NIST SP 800-171. Non-local maintenance must be approved by the system owner in advance.
- **Secure Channels**: Non-local maintenance must be conducted using secure communication methods and must be logged.
- **Documentation Requirement**: Logs must include the names of external personnel, actions performed, time, and any system changes.

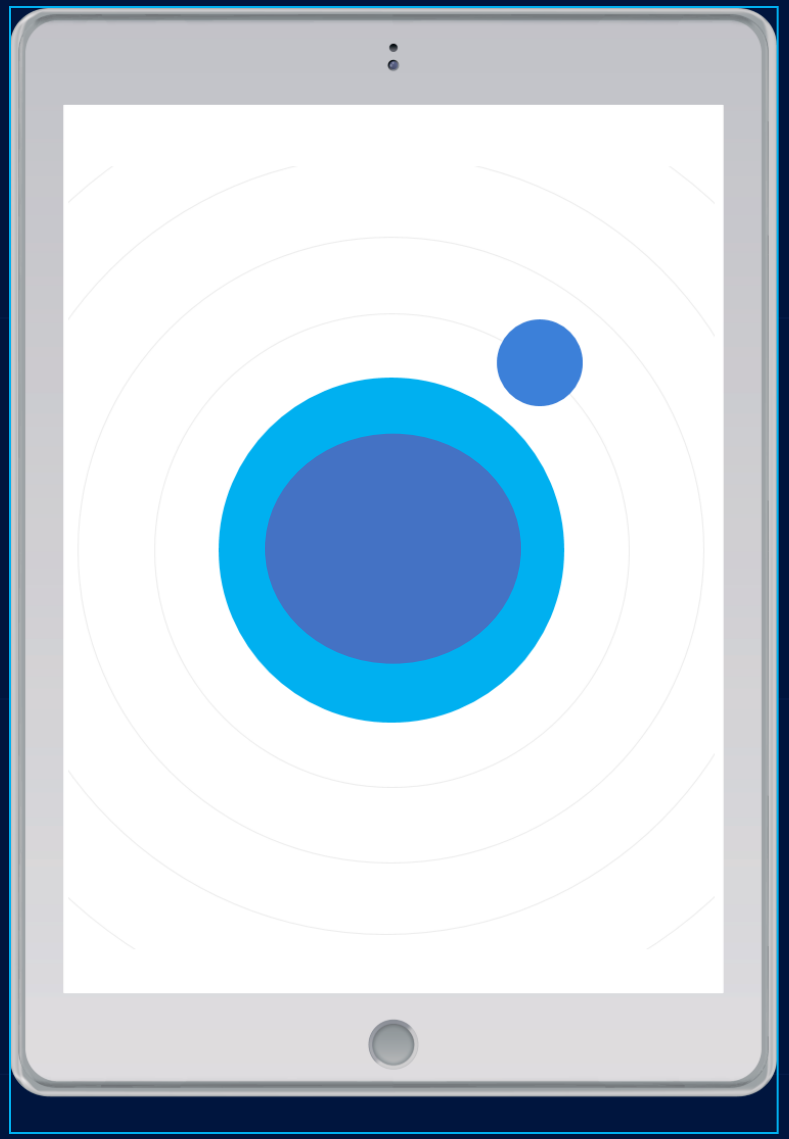


3.5 Personnel Requirements (3.7.5)

•Maintenance personnel must be qualified, authorized, and have appropriate security clearances.

- **Background Checks**: All personnel performing maintenance must undergo appropriate background checks as required by the organization.
- **Training**: Personnel must receive training on secure maintenance practices and understand how to protect CUI during maintenance activities.
- **Access Controls**: Ensure that maintenance personnel have access only to the systems they are authorized to work on.

Elements of the Policy

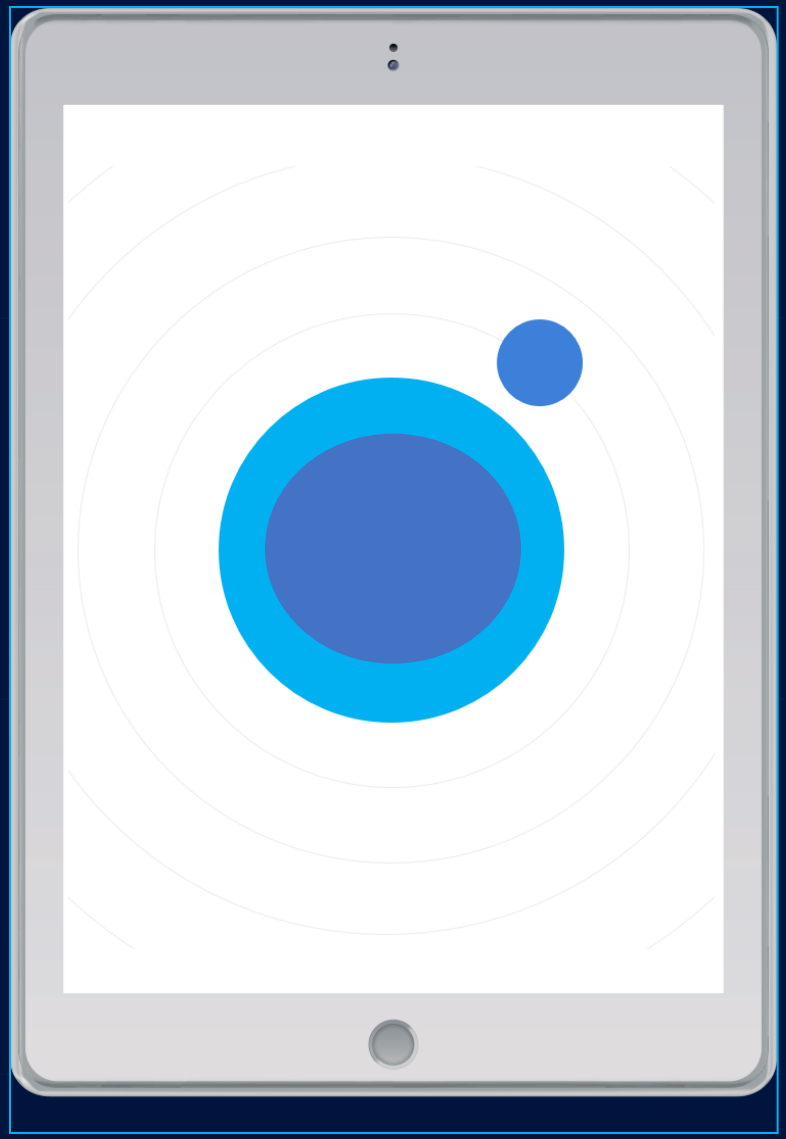


3.6 Maintenance Records (3.7.6)

•Detailed records must be maintained for all maintenance activities.

- **Logs**: Maintenance logs must record:
  - Date and time of the activity.
  - Personnel involved (internal and external).
  - Tools used.
  - System components affected.
  - Description of the tasks performed.
- **Review Process**: Logs must be reviewed regularly to ensure compliance with security protocols.
- **Retention**: Maintenance logs must be retained according to the organization’s data retention policy and must be accessible for audit purposes.

Elements of the Policy

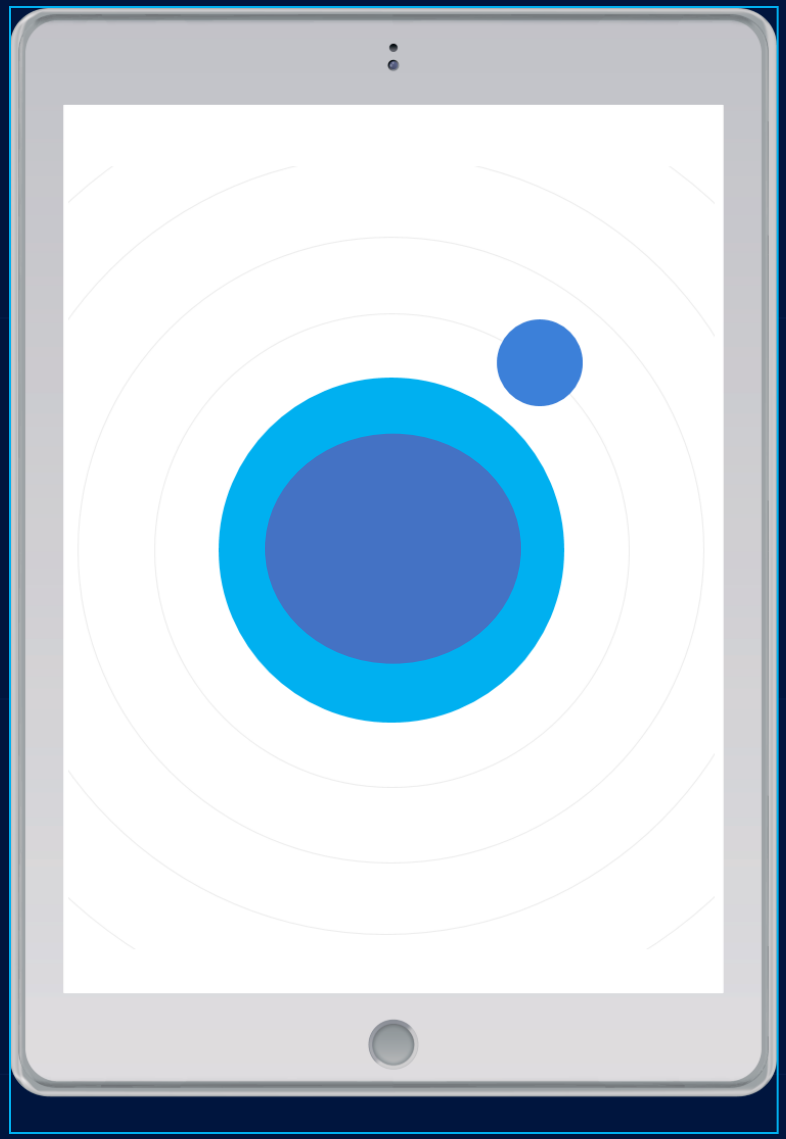


3.7.6	**SECURITY REQUIREMENT** Supervise the maintenance activities of maintenance personnel without required access authorization.
	ASSESSMENT OBJECTIVE *Determine if maintenance personnel without required access authorization are supervised during maintenance activities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System maintenance policy; procedures addressing maintenance personnel; service provider contracts; service-level agreements; list of authorized personnel; maintenance records; access control records; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system maintenance responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for authorizing and managing maintenance personnel; mechanisms supporting or implementing authorization of maintenance personnel].

Elements of the Policy

4. Procedures

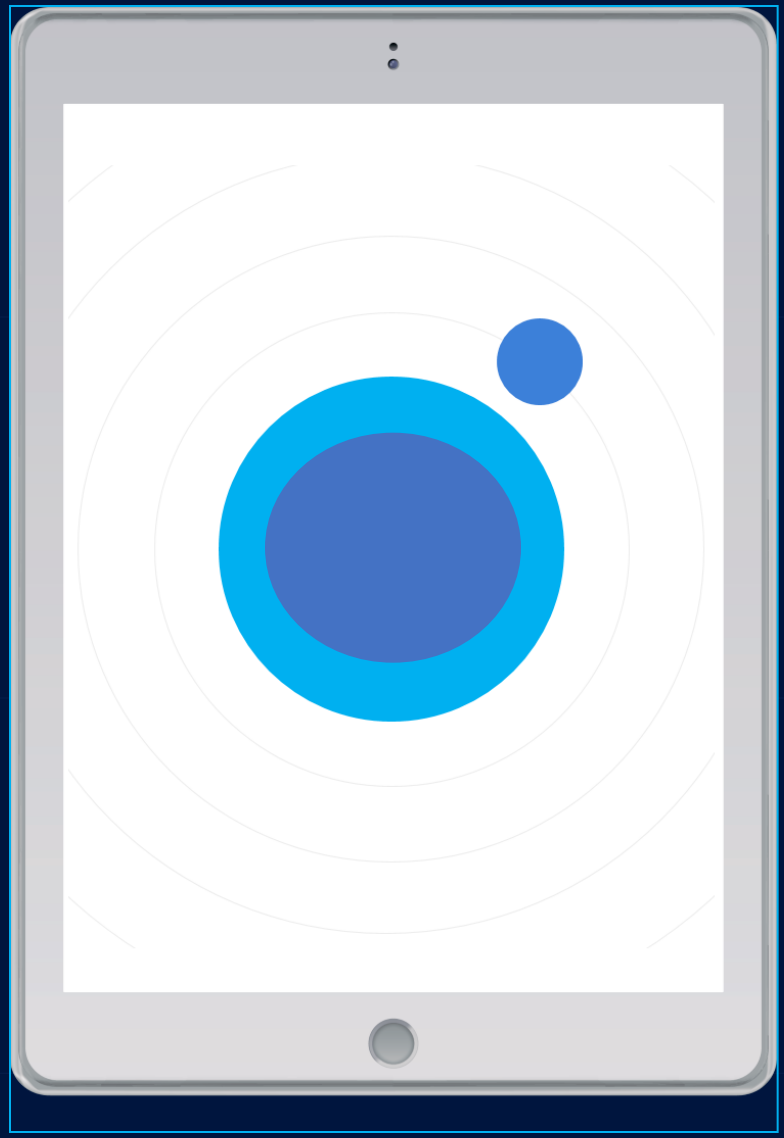
- **Pre-Maintenance Approval**:
  - All maintenance activities must be scheduled and approved in advance by the system owner.
  - Emergency maintenance must follow incident response protocols and be documented immediately after completion.
- **Tool Validation**:
  - All tools used in maintenance must be validated and approved by the cybersecurity team before use.
  - Only authorized personnel are permitted to access and use these tools.
- **Access Control and Monitoring**:
  - Systems involved in maintenance must have restricted access during the activity.
  - Remote and non-local maintenance activities must be monitored by IT staff in real time.
- **Post-Maintenance Review**:
  - After the maintenance activity, the system owner must review the maintenance logs to ensure all tasks were performed in compliance with this policy.
  - Any incidents, vulnerabilities, or security concerns arising during maintenance must be reported to the cybersecurity team.



5. Compliance and Enforcement

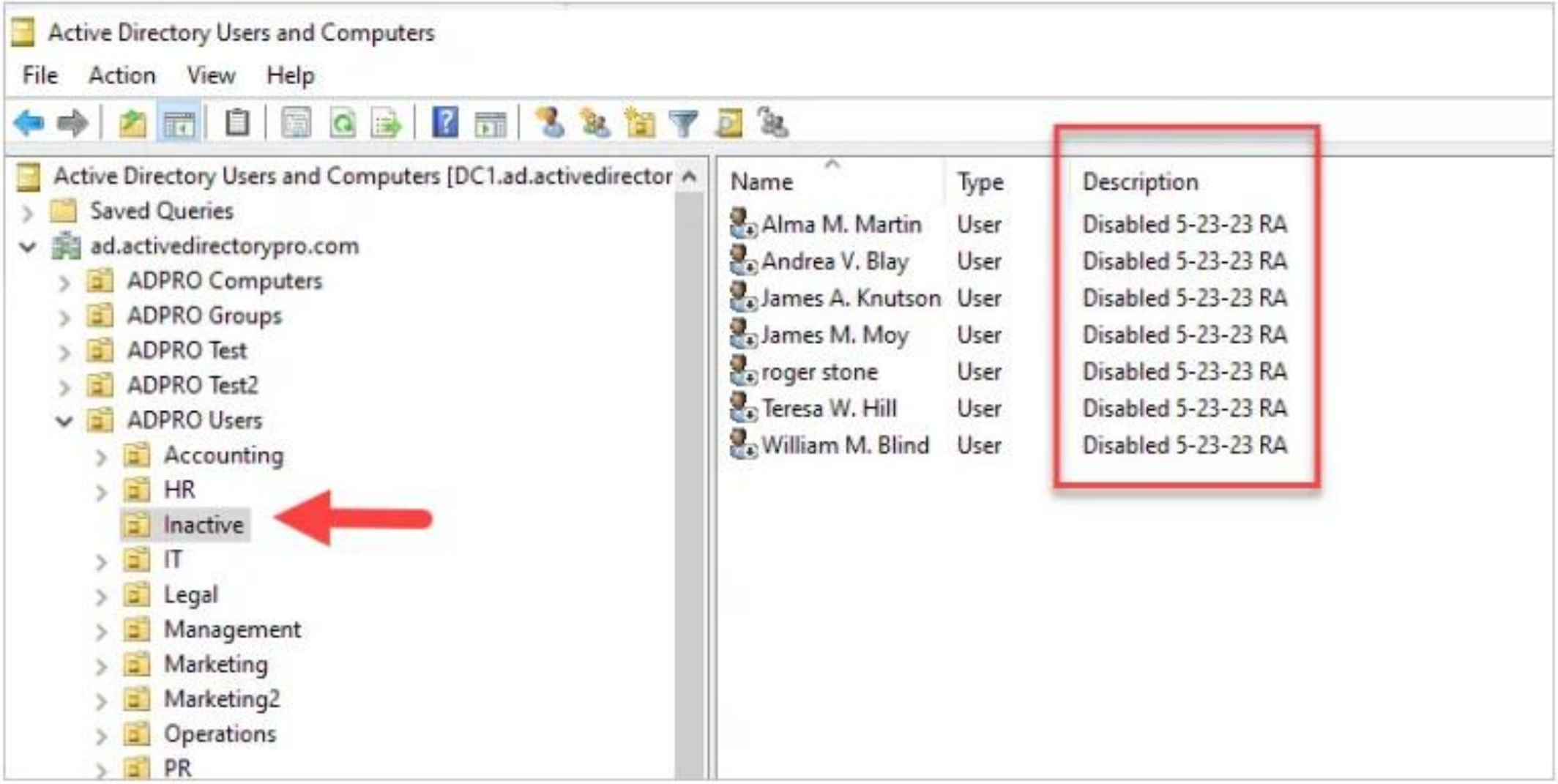
- **Compliance**:
  - All personnel and third-party vendors must comply with this policy.
  - Non-compliance with the policy may result in disciplinary actions or termination of vendor contracts.
- **Auditing**:
  - Regular audits will be conducted to ensure adherence to maintenance procedures and documentation requirements.
- **Incident Response**:
  - Any security incidents or breaches identified during maintenance activities must follow the organization's incident response plan, including reporting, containment, and remediation.

Elements of the Policy

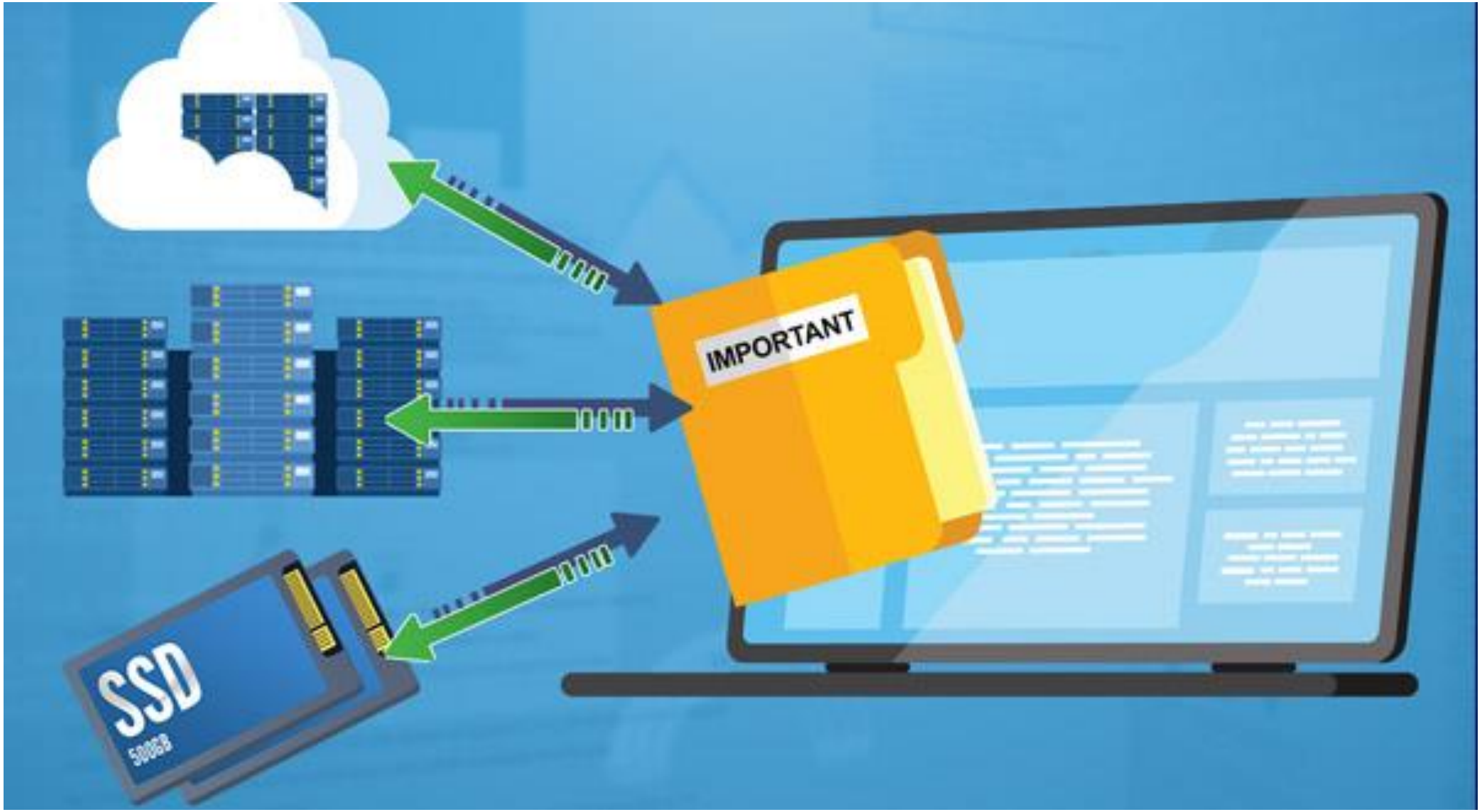


Common Maintenance Processes

Common Maintenance Processes



Common Maintenance Processes

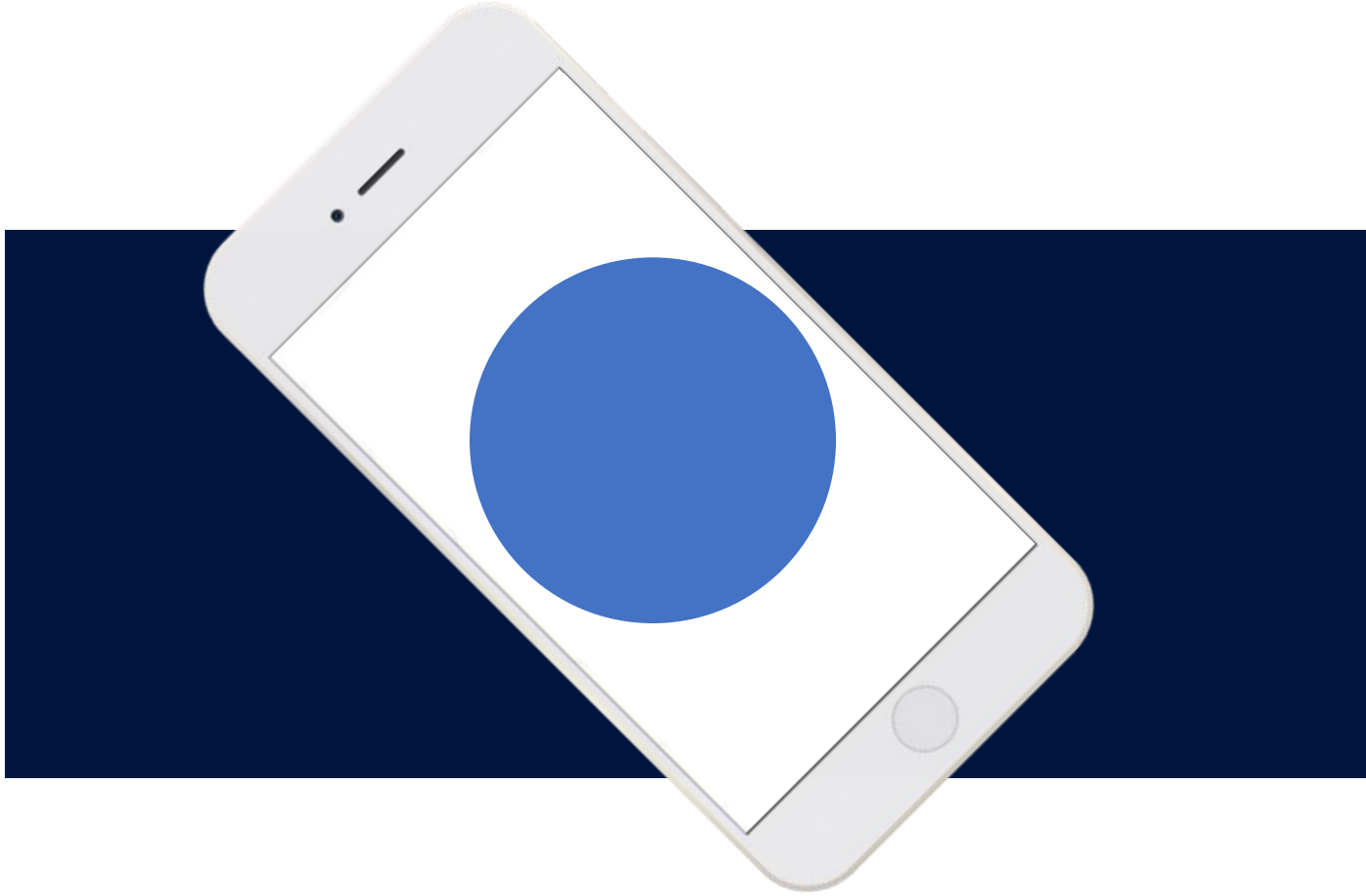


Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

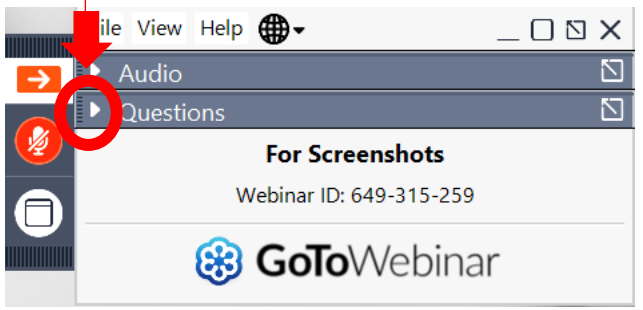
AN APEX ACCELERATOR



QUESTIONS?

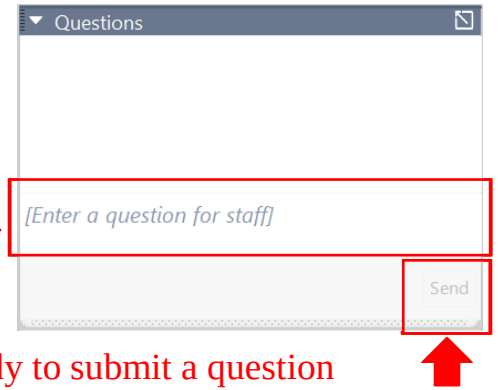
OPENING THE QUESTIONS BOX

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.

- **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

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

EMERGING ISSUES WEBINAR SERIES

This series is intended as an information tool and resource for contract managers and those with a compliance function. Attendees receive 1 CPE credit for attending.

- ~~**Aug 22 –** Regulation Making – The Process and the Important Role Businesses Play~~
- ~~**Sep 19 –** Industry 4.0 – The Next Generation of the DIB~~
- **Oct 24** – Innovation – What Does Innovation Look Like from DoD's Perspective?
- **Nov 21** – The Critical Role Your Accounting System Plays in SBIR/STTR Success

Wisconsin Procurement Institute
An APEX Accelerator

…More information and registrations at wispro.org/events

- Save the Date -

The Contracting Academy

Developing and Growing Government Contractors

Dec 10

Virtual | 9:00 am - 4:00 pm

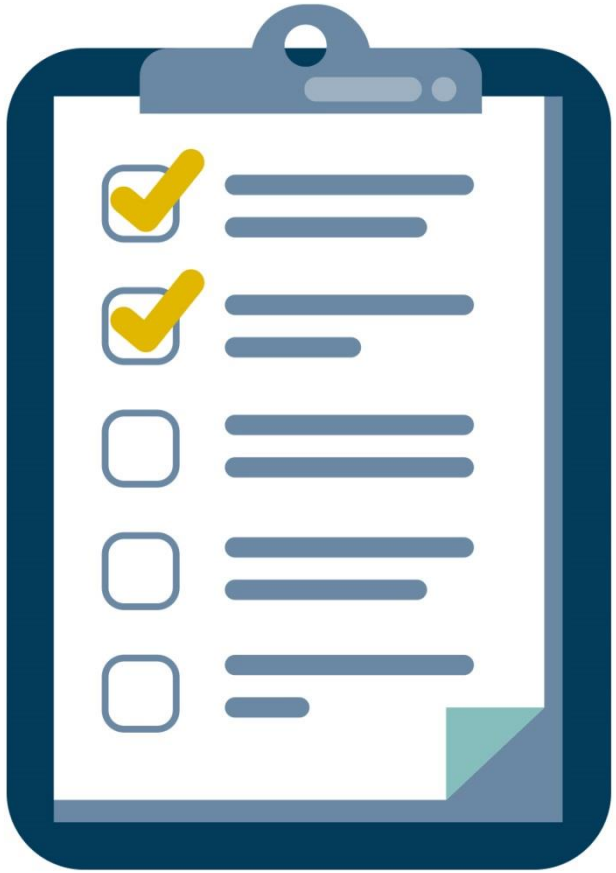
The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…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

October 18, 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 | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226