Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:
3.1.8 Media Control Policy, Media Destruction Policy and Personnel Security

November 22 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

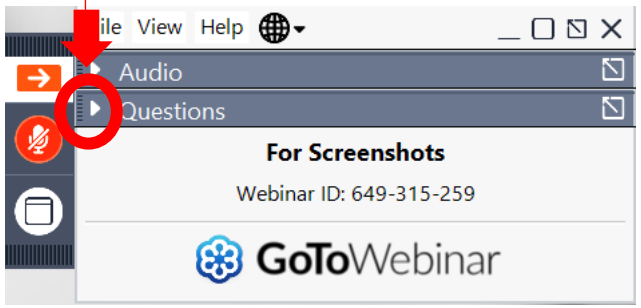
PLEASE

- 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!

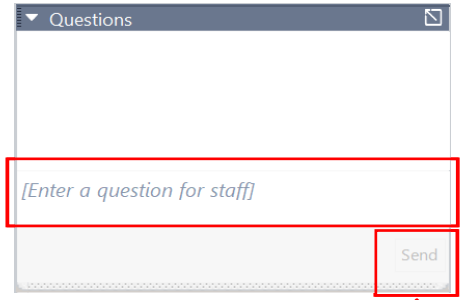
OPENING THE QUESTIONS BOX

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.

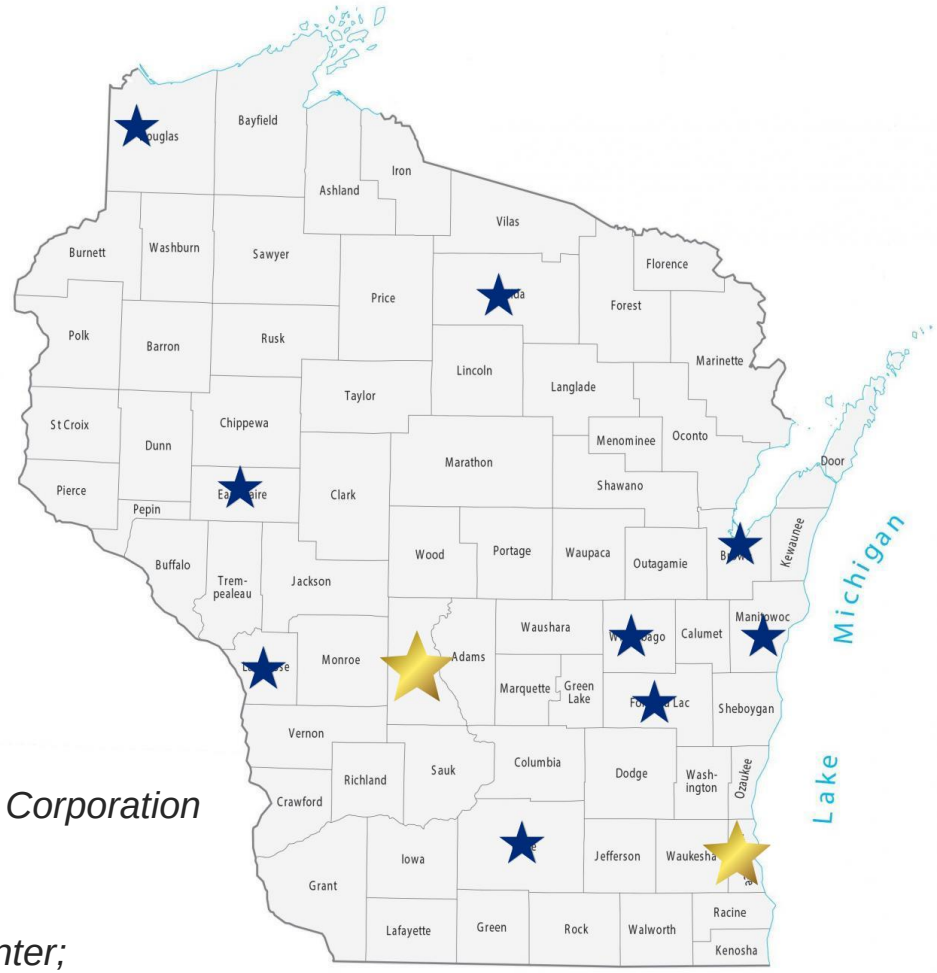
WPI provides services to all of Wisconsin's 72 counties

- 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……

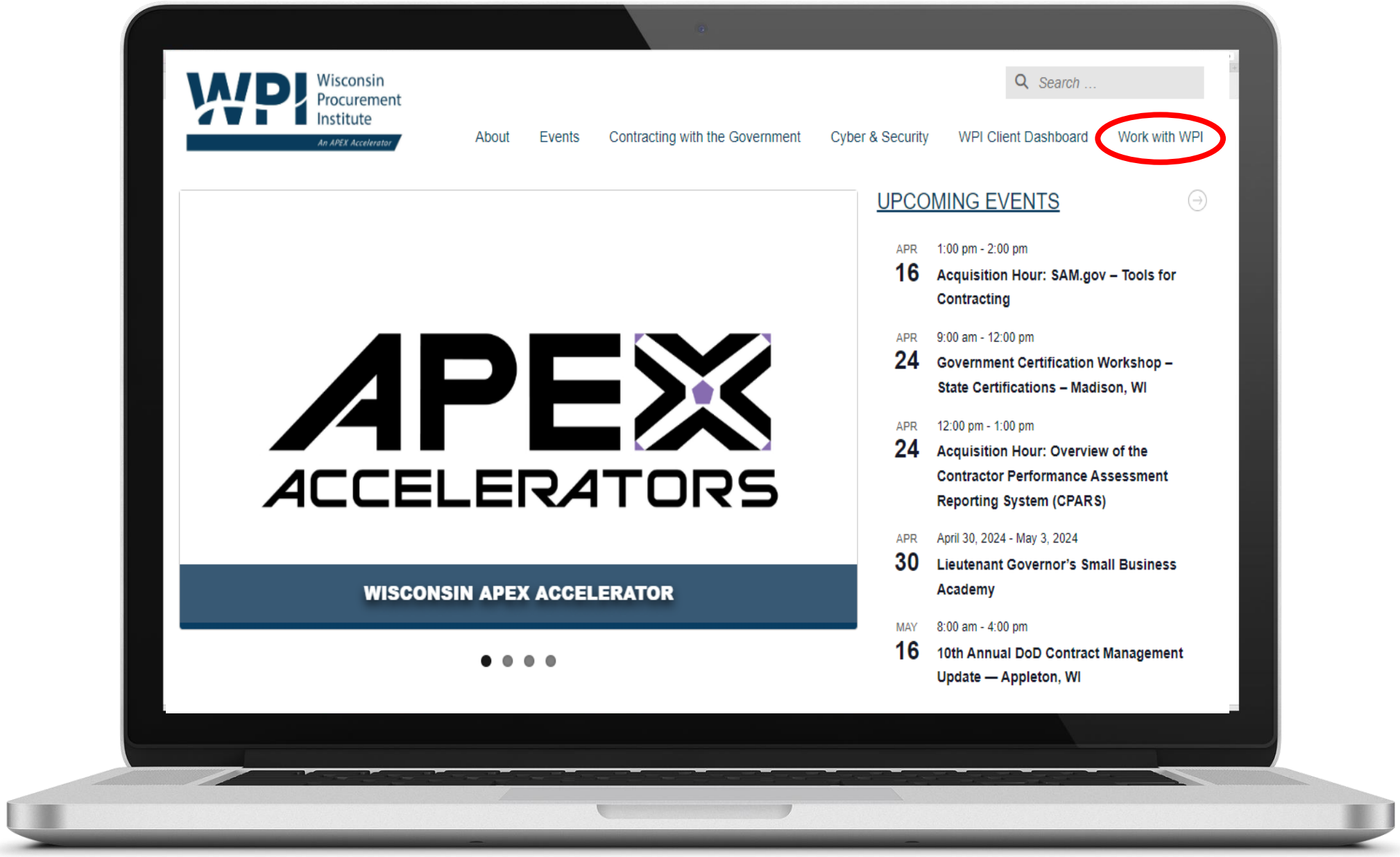
www.wispro.org

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*



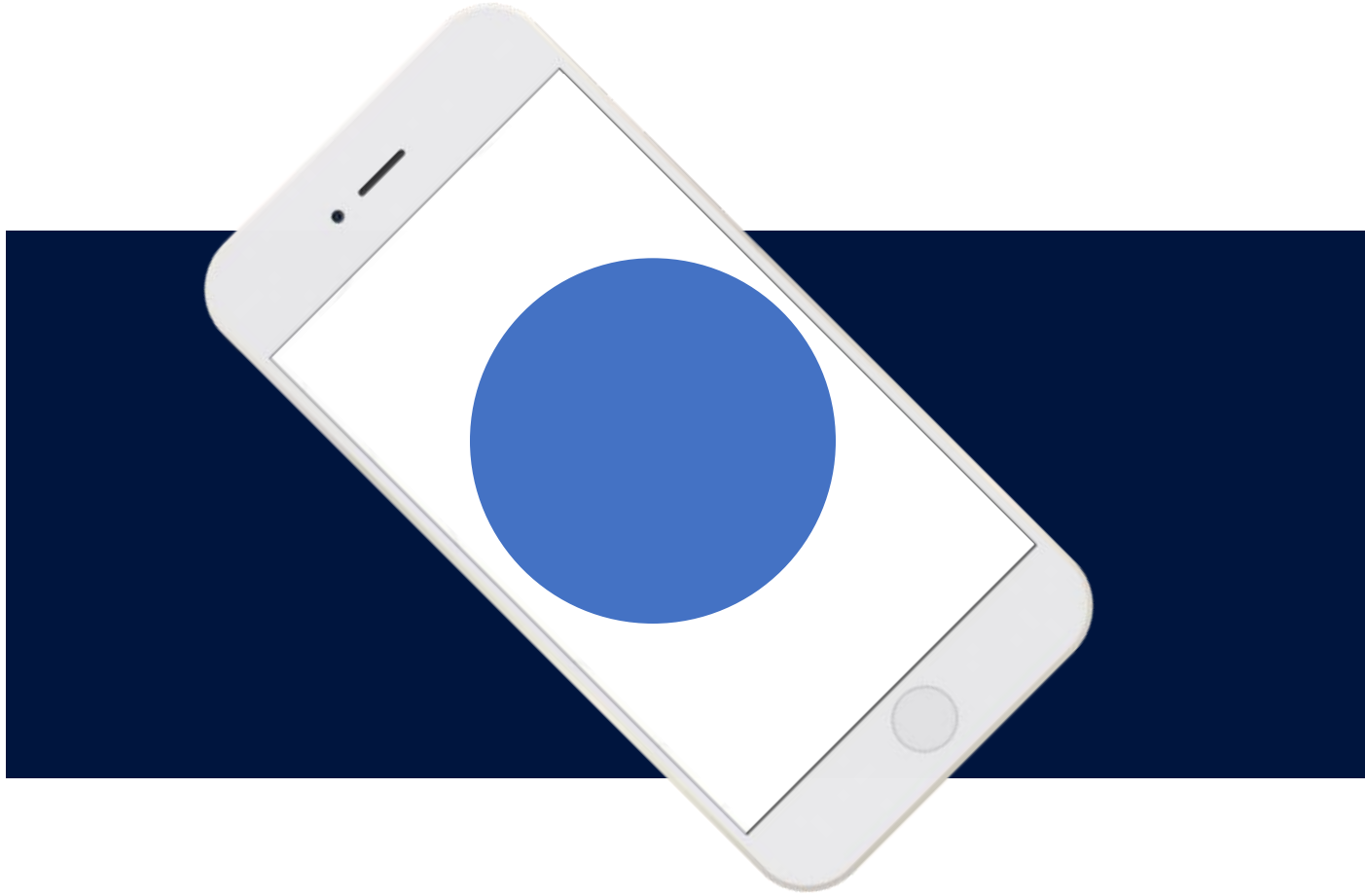
Wisconsin Procurement Institute
An APEX Accelerator


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.

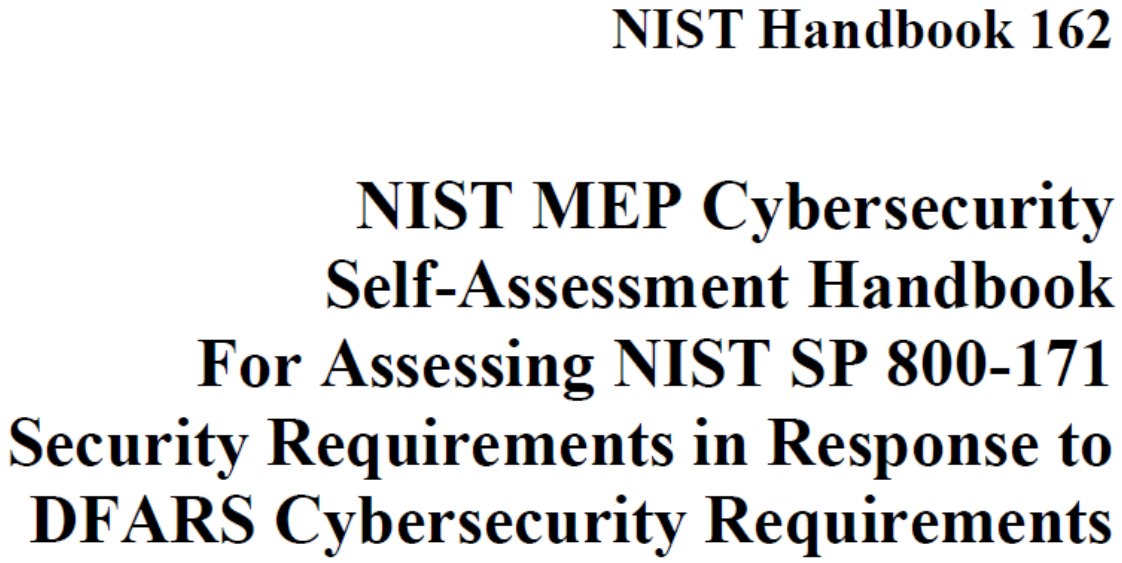
DFARS 252.204-7021

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

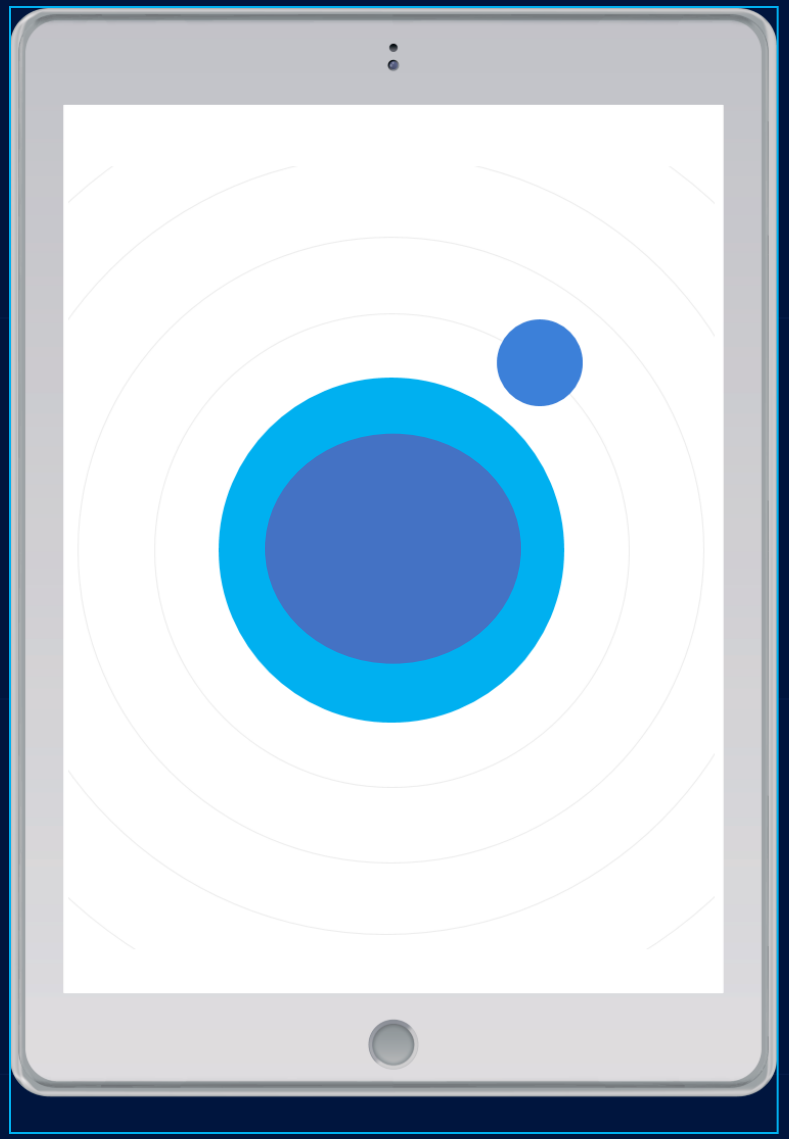
3 NIST SP 800-18r1

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

Media Control

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
    - Media Custodians
    - IT Personnel/Administrators
    - Security/Compliance Officer
    - All Personnel



Incident Response Team

Media Custodian

- ❑ Usage
- ❑ Accountability

IT Personnel/Admins

- ❑ Configuration
- ❑ Labelling
- ❑ Provisioning

Security/Compliance

- ❑ Validation of Process

All Personnel

- ❑ Safe Handling
- ❑ Incident Reporting

3.8.1	**SECURITY REQUIREMENT** Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.8.1[a] *paper media containing CUI is physically controlled.*
	3.8.1[b] *digital media containing CUI is physically controlled.*
	3.8.1[c] *paper media containing CUI is securely stored.*
	3.8.1[d] *digital media containing CUI is securely stored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System media protection policy; procedures addressing media storage; procedures addressing media access restrictions; access control policy and procedures; physical and environmental protection policy and procedures; system security plan; media storage facilities; access control records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system media protection responsibilities; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Organizational processes for restricting information media; mechanisms supporting or implementing media access restrictions].

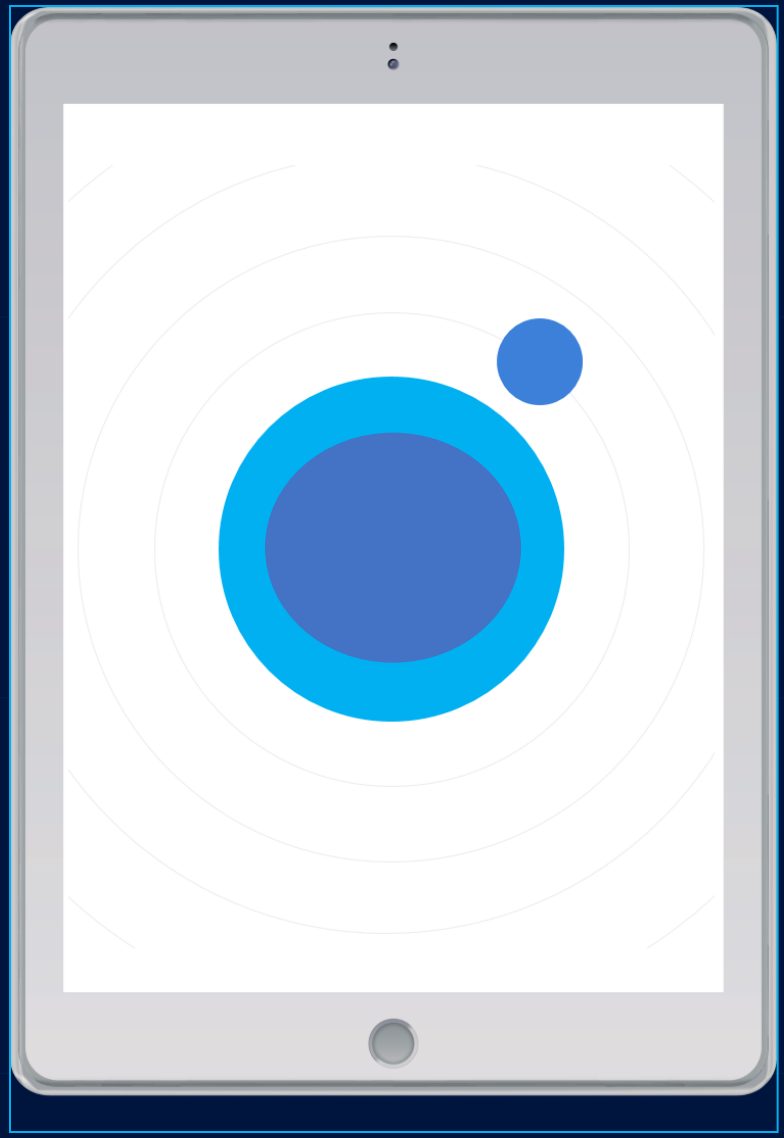
3. Policy Statements

3.1 Media Protection

•Digital and Physical Media will have appropriate controls.

- **Physical Media**: All media containing CUI must be clearly labeled and stored in secure locations such as locked cabinets, safes, or secure server rooms with physical access controls.
- **Removable Media**: Portable media must be encrypted using FIPS 140-2 compliant encryption standards when stored or transported. Must be labelled.
- **Cloud-based Media**: Cloud-based media must adhere to encryption and security requirements specified by the Federal Risk and Authorization Management Program (FedRAMP).

Elements of the Policy



CUI

ATTENTION

Use this space to indicate categories, limited dissemination controls, special instructions, points of contact, etc., if needed.

ATTENTION

All individuals handling this information are required to protect it from unauthorized disclosure.

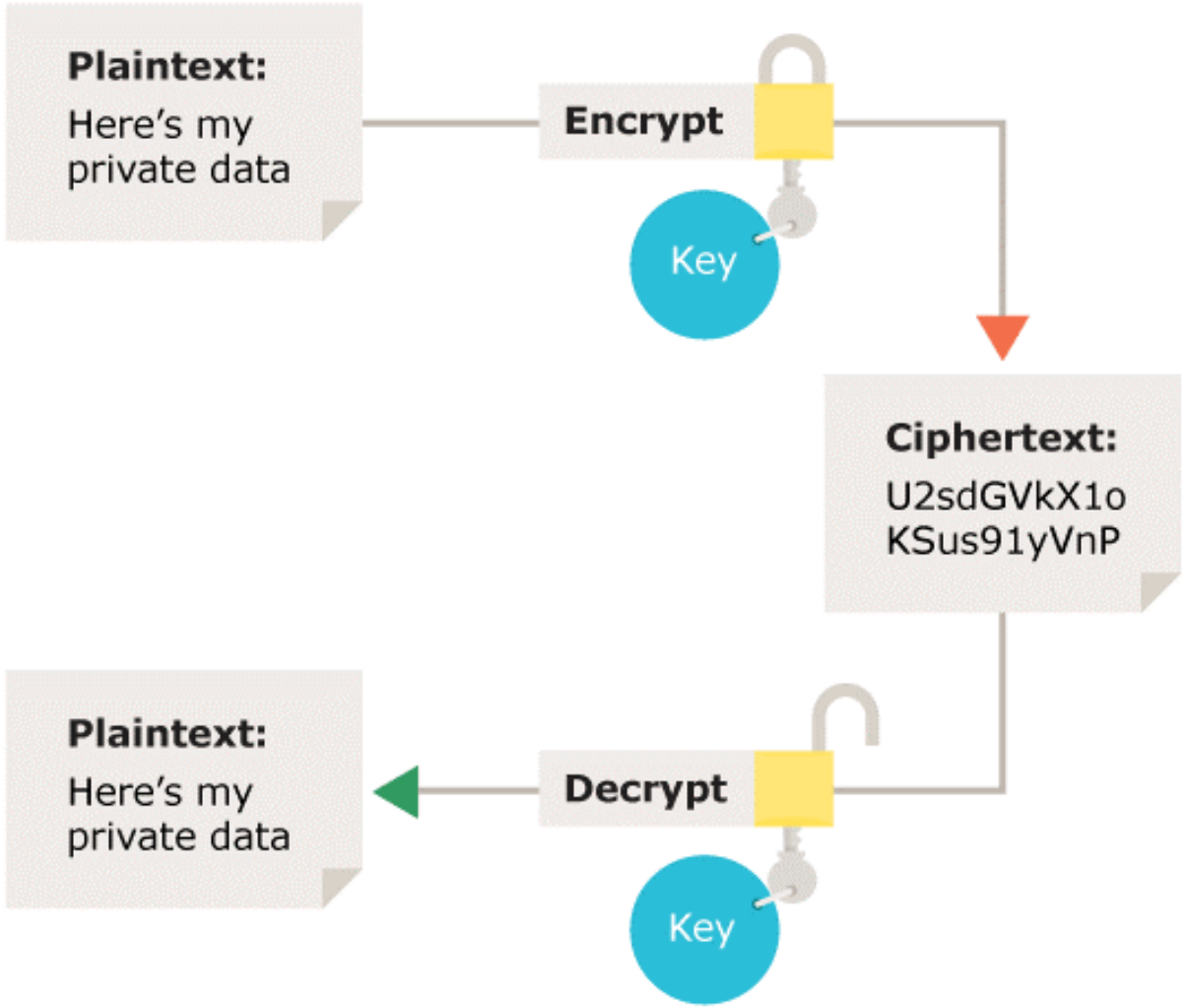
Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

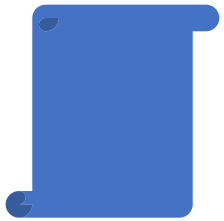
CUI

3.8.6	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
	ASSESSMENT OBJECTIVE *Determine if the confidentiality of CUI stored on digital media is protected during transport using cryptographic mechanisms or alternative physical safeguards.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System media protection policy; procedures addressing media transport; system design documentation; system security plan; system configuration settings and associated documentation; system media transport records; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system media transport responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Cryptographic mechanisms protecting information on digital media during transportation outside controlled areas].

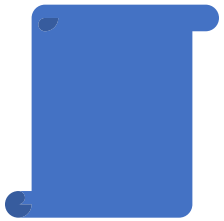
Removable Drive Checkout



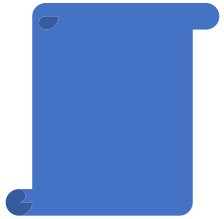
NIST SP 800-171 Encryption At Rest



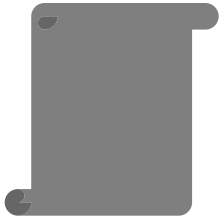
3.1.19 Encrypt CUI on mobile Devices and computing platforms



3.13.11 Employ FIPS-validated Cryptography when used to protect The confidentiality of CUI.



3.13.4 Prevent unauthorized And unintended transfer via Shared system resources.



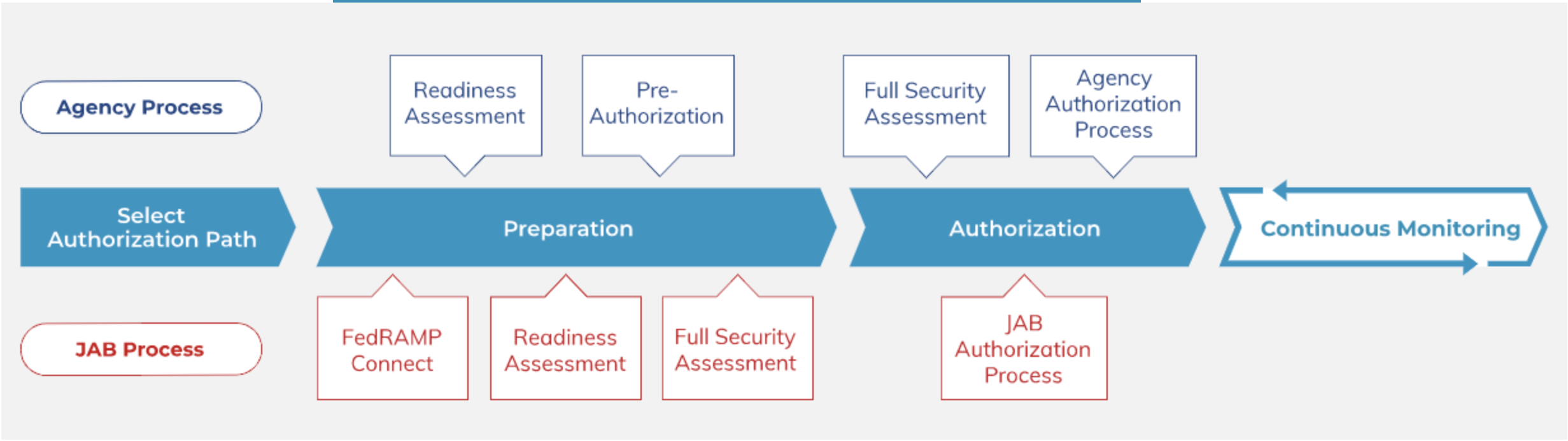
3.13.16 Protect the confidentiality Of CUI at rest.

What is FedRAMP?

SECURING CLOUD SERVICES

FOR THE FEDERAL GOVERNMENT

The Federal Risk and Authorization Management Program (FedRAMP®) provides a standardized approach to security authorizations for Cloud Service Offerings.



Cloud Providers

Which Cloud Providers are FedRAMP Certified?

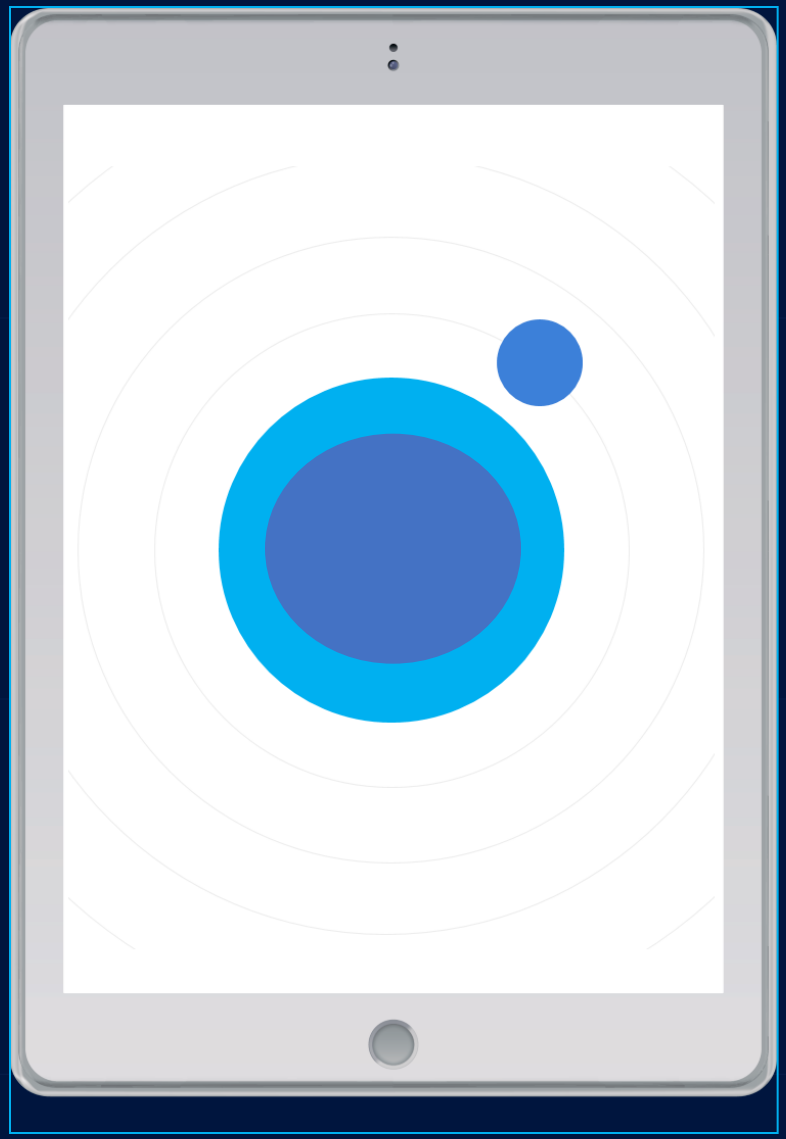
As of today, more than 250 FedRAMP-certified vendors are listed on the FedRAMP Marketplace. Remember, however, that it's the service – not the service provider – that gets authorized. This means a CSP may have to pursue multiple authorizations if it offers more than one cloud-based solution.

3.13.2	**SECURITY REQUIREMENT** Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.13.2[a]	*architectural designs that promote effective information security are identified.*
	3.13.2[b]	*software development techniques that promote effective information security are identified.*
	3.13.2[c]	*systems engineering principles that promote effective information security are identified.*
	3.13.2[d]	*identified architectural designs that promote effective information security are employed.*
	3.13.2[e]	*identified software development techniques that promote effective information security are employed.*

3.13.8	**SECURITY REQUIREMENT** Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.8[a] *cryptographic mechanisms intended to prevent unauthorized disclosure of CUI are identified.*
	3.13.8[b] *alternative physical safeguards intended to prevent unauthorized disclosure of CUI are identified.*
	3.13.8[c] *either cryptographic mechanisms or alternative physical safeguards are implemented to prevent unauthorized disclosure of CUI during transmission.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System and communications protection policy; procedures addressing transmission confidentiality and integrity; system security plan; system design documentation; system configuration settings and associated documentation; 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:* Cryptographic mechanisms or mechanisms supporting or implementing transmission confidentiality; organizational processes for defining and implementing alternative physical safeguards].

"If it is infeasible or impractical to obtain the necessary safeguards and assurances of the effectiveness of the safeguards through appropriate contracting vehicles, organizations implement **compensating safeguards** or explicitly accept the additional risk."

Control Language



3.8.2	**SECURITY REQUIREMENT** Limit access to CUI on system media to authorized users.
	ASSESSMENT OBJECTIVE *Determine if access to CUI on system media is limited to authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system media protection and storage responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

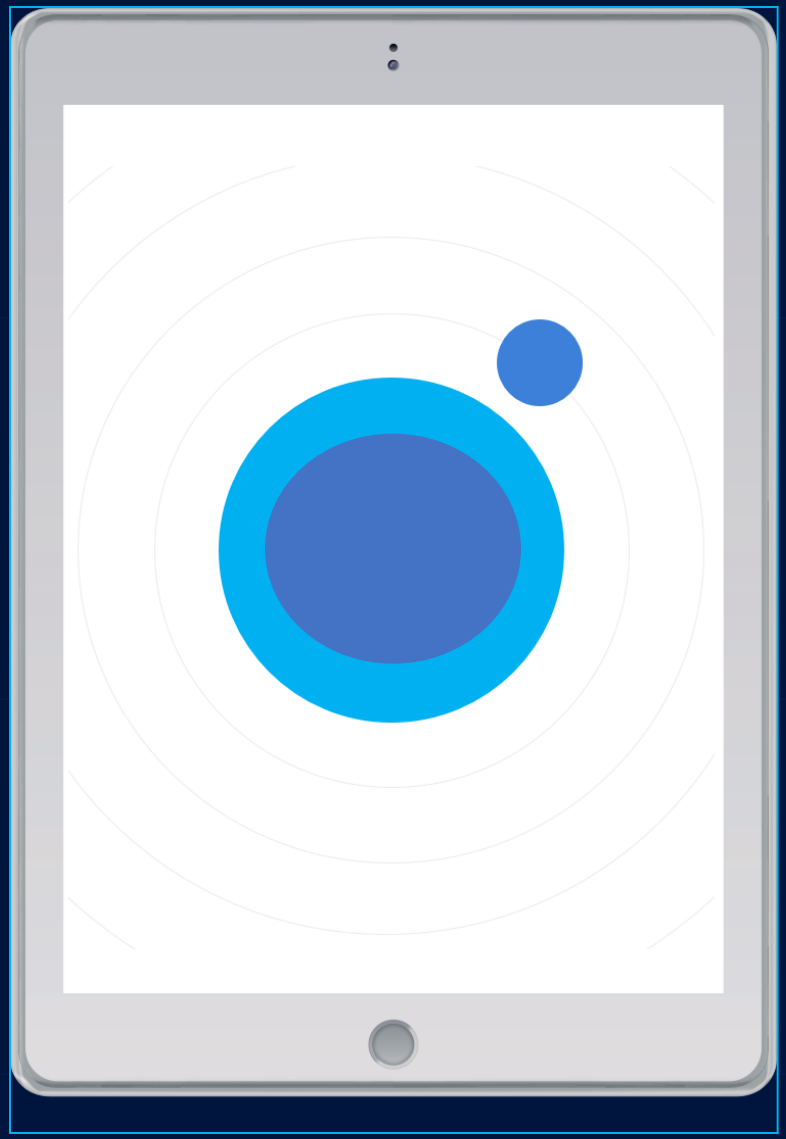
3. Policy Statements

3.2 Media Access Controls

•Only qualified and authorized personnel are approved to have access to media containing CUI.

- **Media Custodians**: Maintain accountability and authority over all pieces of removable media at use in the environment.
- **IT Personnel**: Ensure removable media, if digital, is configured for the proper handling of CUI.
- **Compliance Personnel**: Validates authorized procedures and processes are being followed to ensure compliance.

Elements of the Policy



3.8.3	**SECURITY REQUIREMENT** Sanitize or destroy system media containing CUI before disposal or release for reuse.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.8.3[a]	*system media containing CUI is sanitized or destroyed before disposal.*
	3.8.3[b]	*system media containing CUI is sanitized before it is released for reuse.*

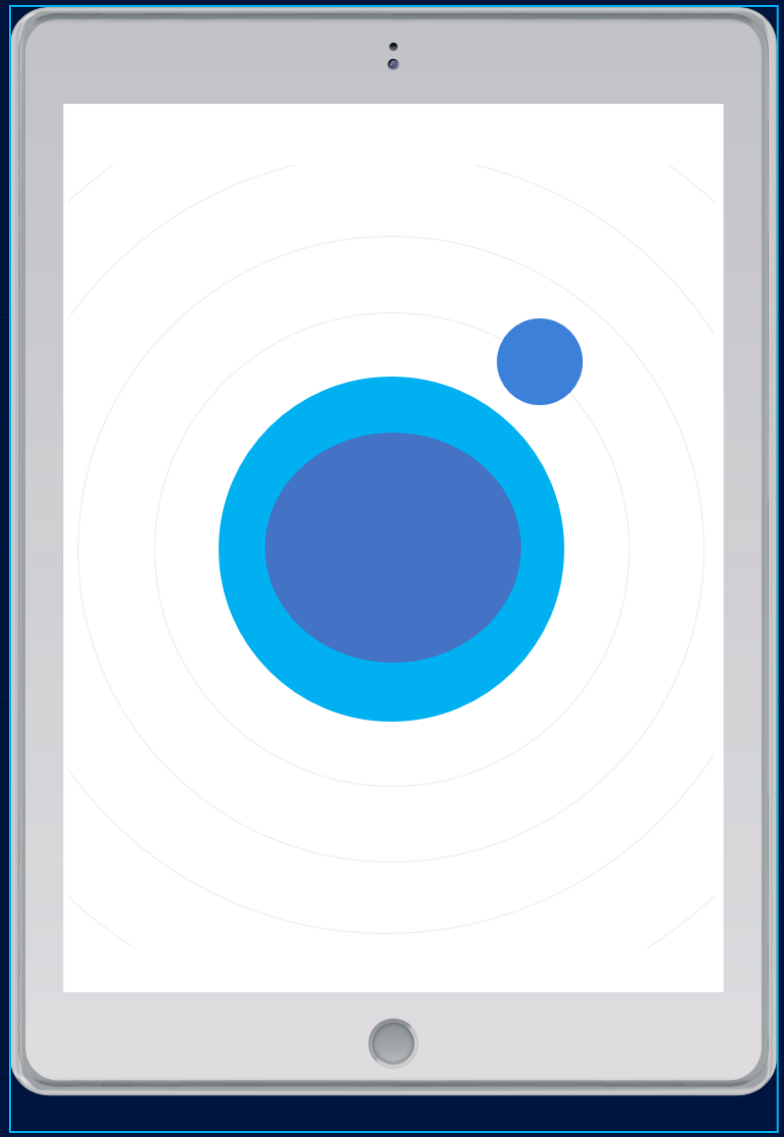
3. Policy Statements

3.3 Media Disposal

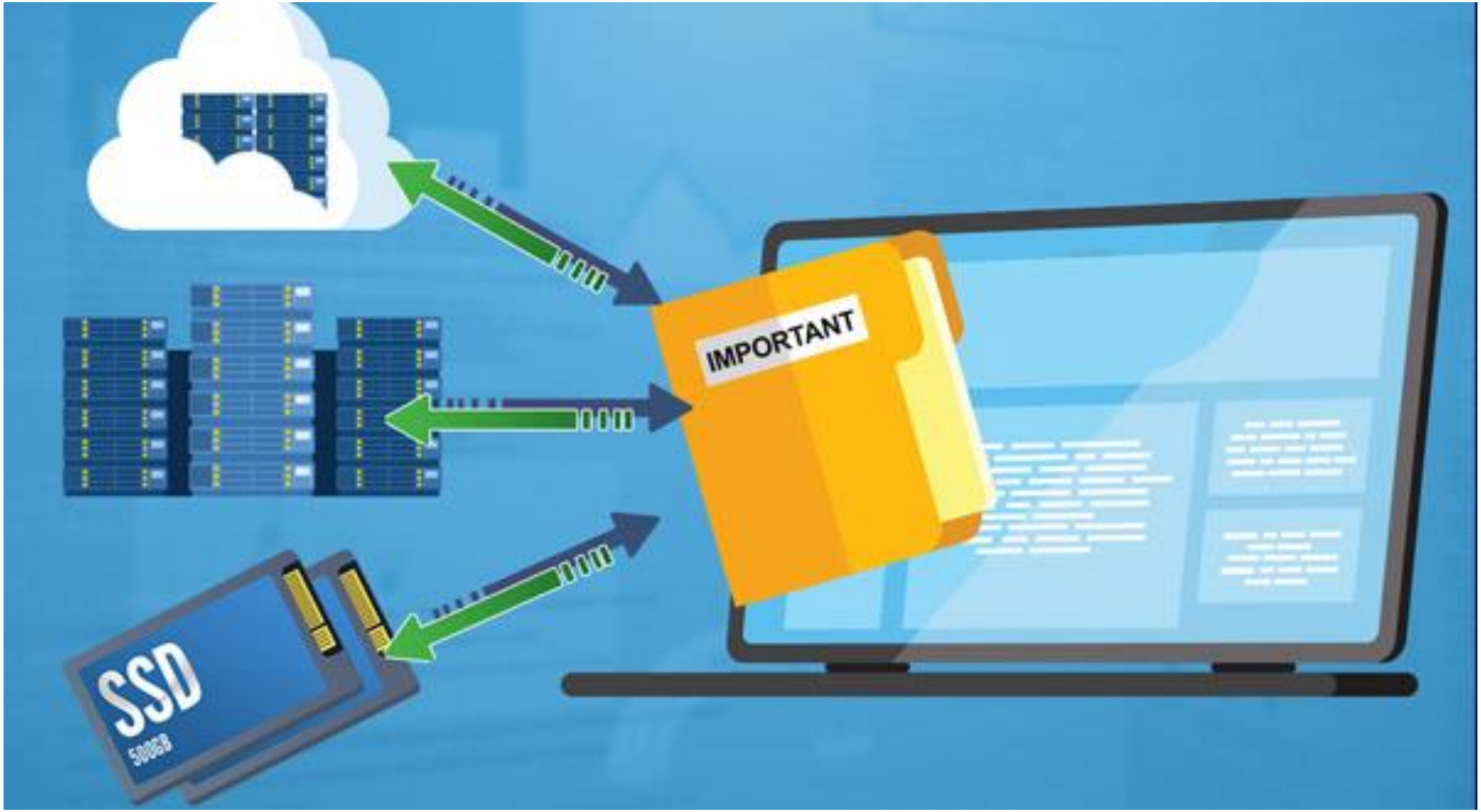
•Media will be appropriately sanitized and destroyed.

- **Secured**: Physical media with CUI must not be discarded in unsecured trash or recycling bins.
- **Record Keeping**: A record of media sanitization and destruction must be maintained, including details such as media type, serial numbers (if applicable), date, and method used.
- **Sanitization**: Media no longer required must be sanitized using approved methods (e.g., DoD 5220.22-M wiping standards, degaussing) or destroyed (e.g., shredding, incineration) before disposal.

Elements of the Policy



Other Media Types



Backup Solutions

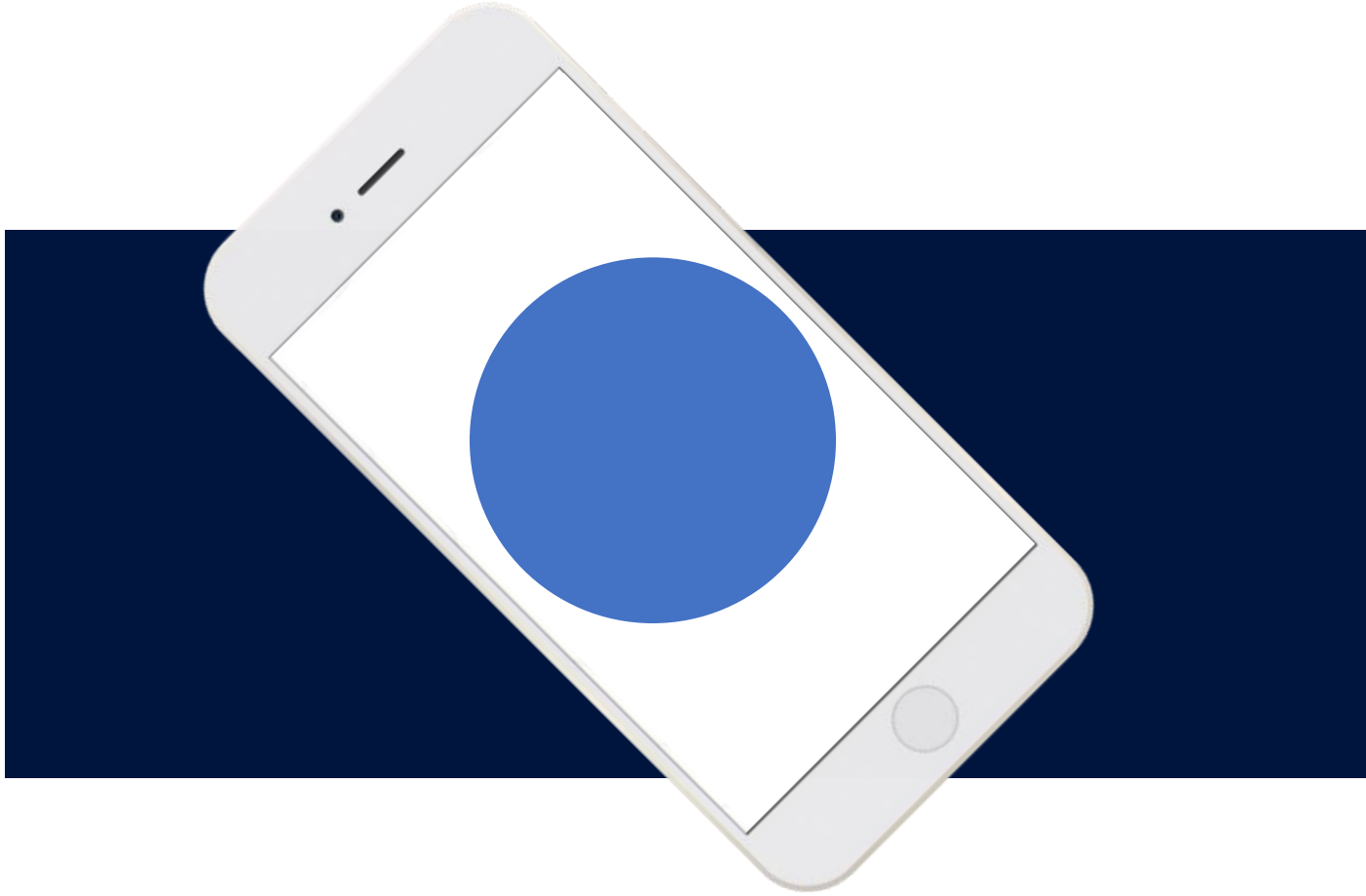
3.8.9	**SECURITY REQUIREMENT** Protect the confidentiality of backup CUI at storage locations.
	ASSESSMENT OBJECTIVE *Determine if the confidentiality of backup CUI is protected at storage locations.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Procedures addressing system backup; system configuration settings and associated documentation; security plan; backup storage locations; system backup logs or records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with system backup responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for conducting system backups; mechanisms supporting or implementing system backups].

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

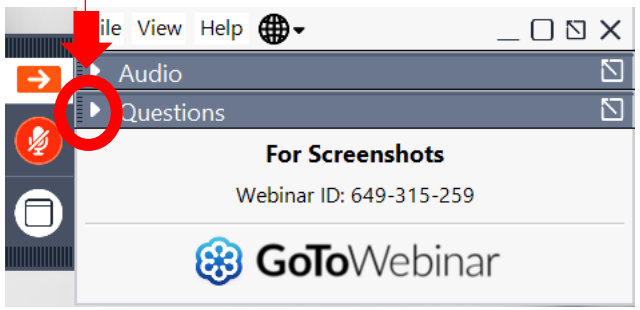
AN APEX ACCELERATOR



QUESTIONS?

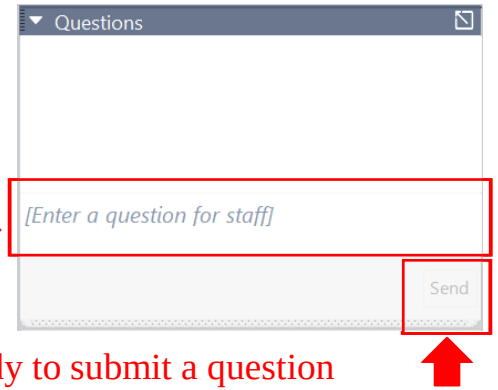
OPENING THE QUESTIONS BOX

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

Wisconsin Procurement Institute
An APEX Accelerator

November 22, 2024

NCMA
NATIONAL CONTRACT MANAGEMENT ASSOCIATION
WISCONSIN

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.

- **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

- 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

Wisconsin Procurement Institute

An APEX Accelerator

Emerging Issues:

The critical role your accounting system plays in SBIR/STTR success

November 21| 11:00 am - Noon

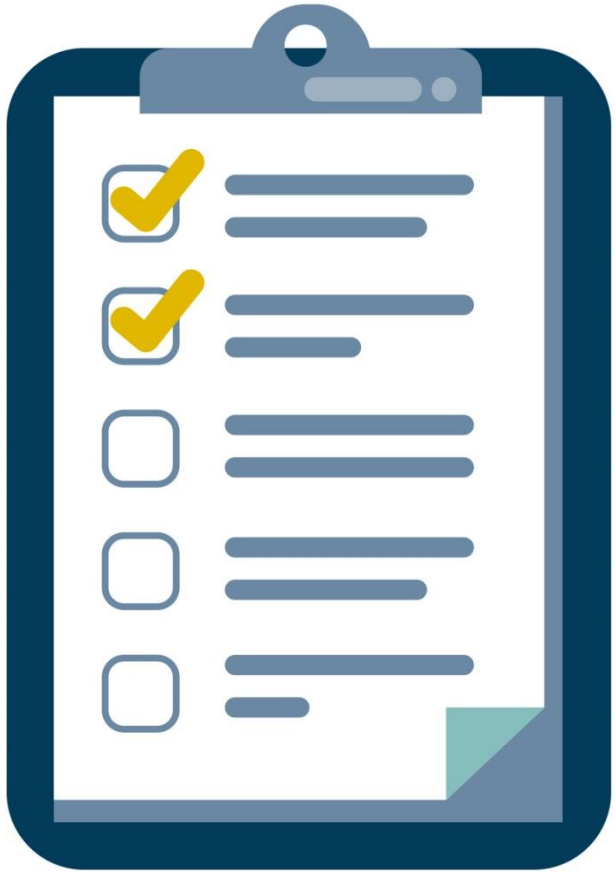
Presented by:

Marc Violante, Wisconsin Procurement Institute

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

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

SURVEY



Wisconsin Procurement Institute
An APEX Accelerator

November 22, 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