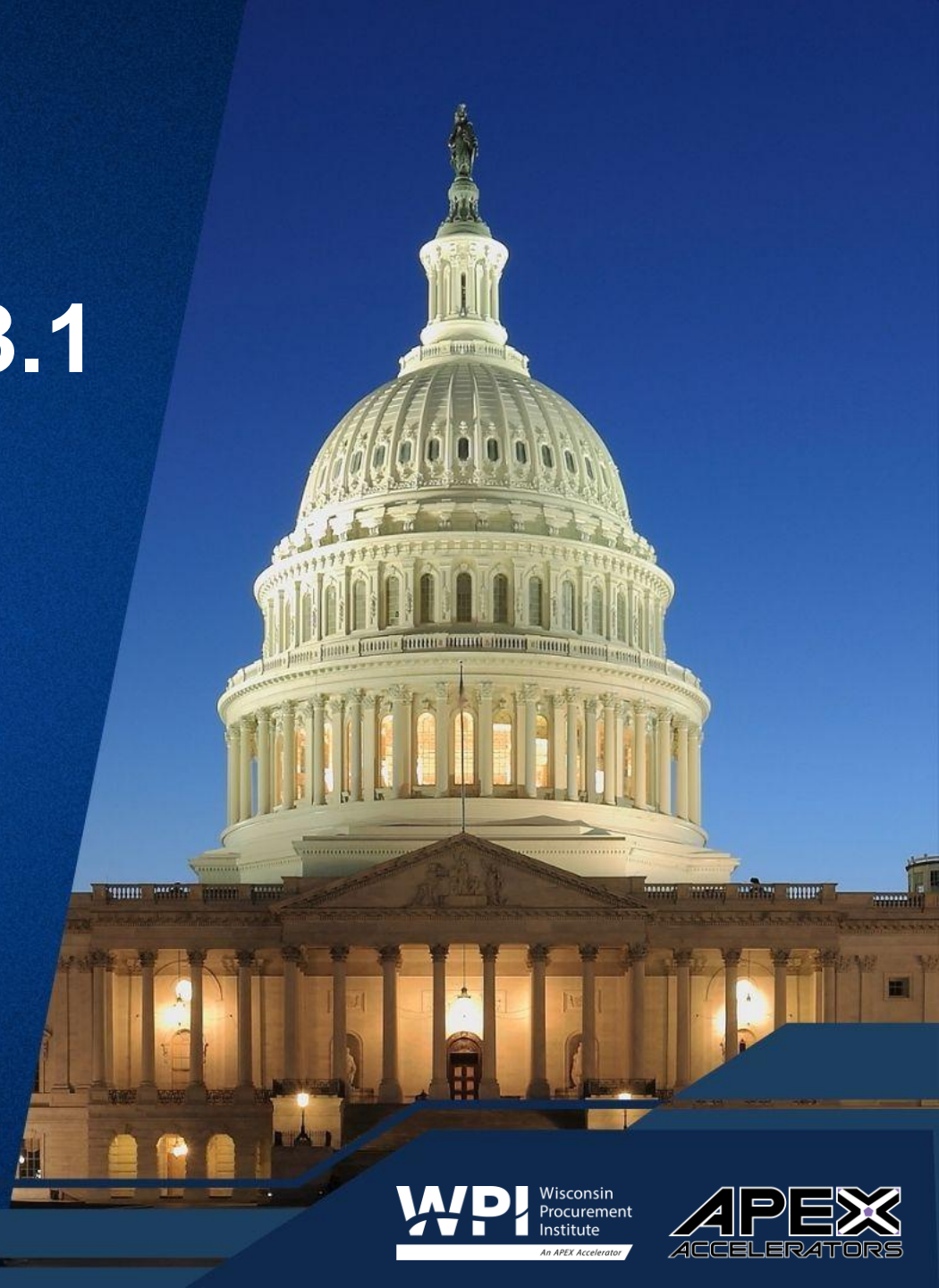
Cyber Thursday:

CMMC: Control Set Series: 3.1 Access Control

February 26| 11:00 am - Noon

Presented by:
Matt Frost, Wisconsin Procurement Institute



WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

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.

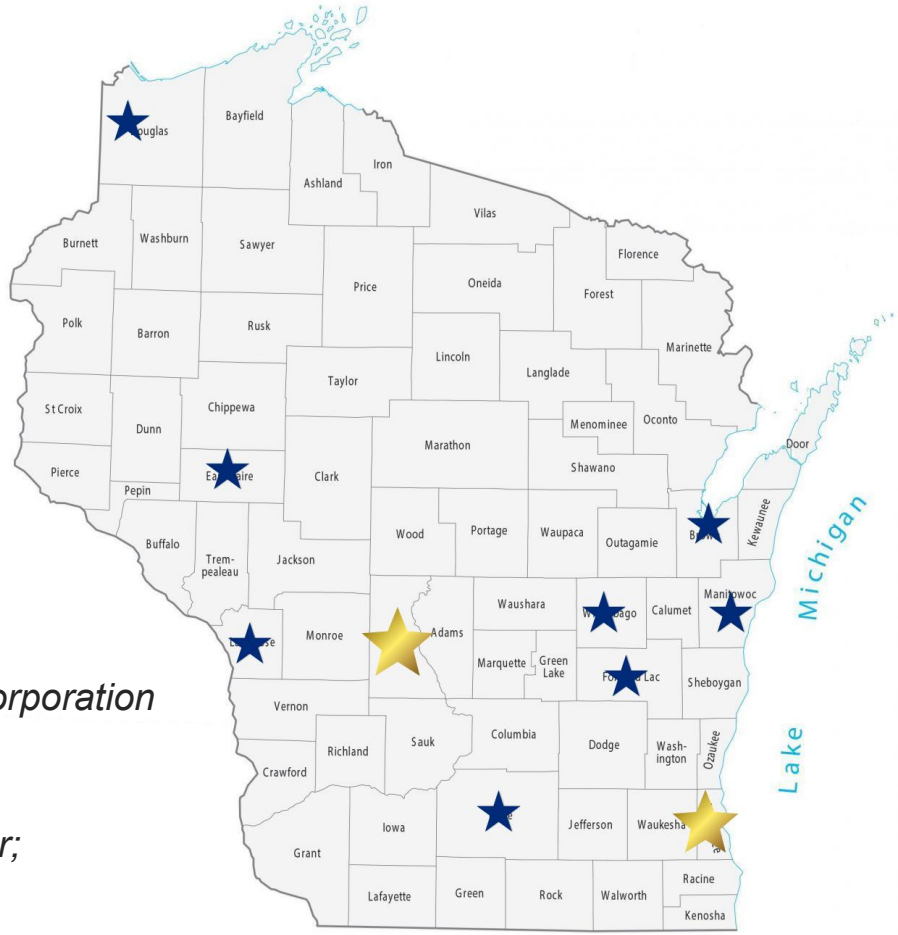
WPI provides services and training to all of Wisconsin's 72 counties

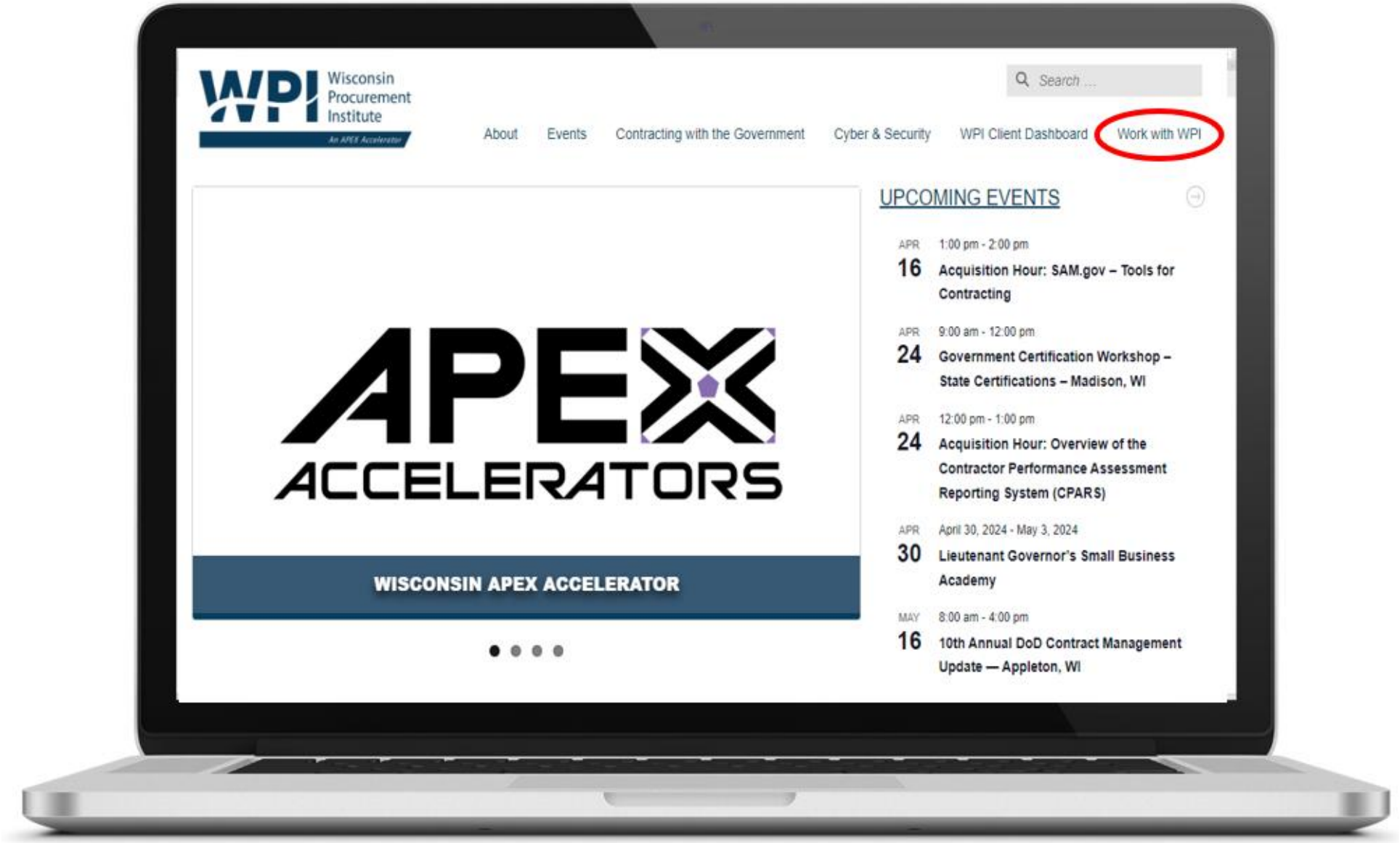
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more……

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *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*

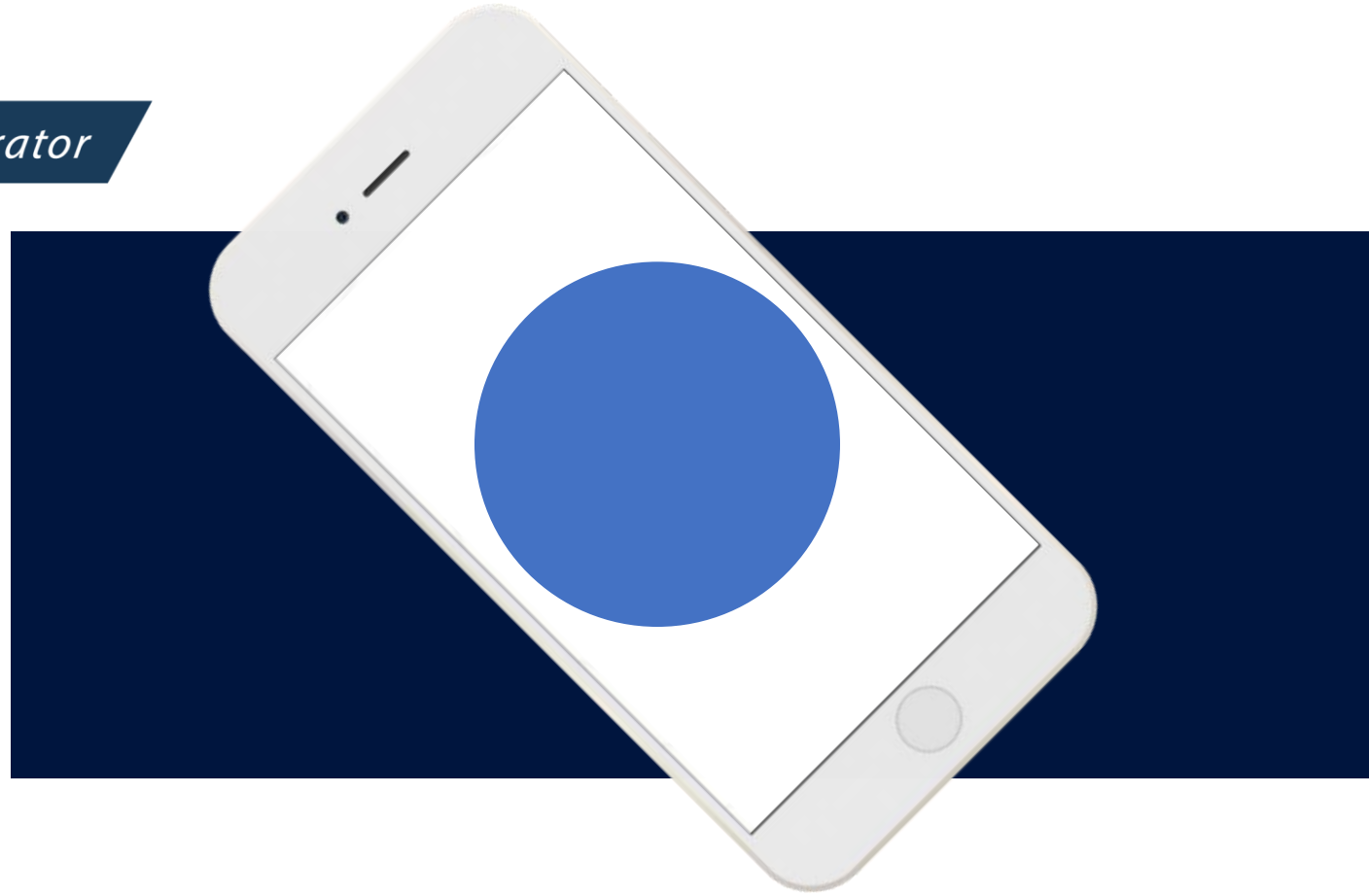



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 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

Wisconsin Procurement Institute

An APEX Accelerator

Access Control



Cyber Thursday – February 26th, 2026


LOCKHEED MARTIN
3103

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

ABOUT US ▾ ACCREDITATION ▾ RESOURCES ▾ CMMC ECOSYSTEM ▾ NEWS & EVENTS ▾ MARKETPLACE CAICO

www.cyberab.org

Access Control (AC)..... 12

Level 1 AC Practices 12

AC.L1-3.1.1 – Authorized Access Control 12

AC.L1-3.1.2 – Transaction & Function Control 14

AC.L1-3.1.20 – External Connections..... 16

AC.L1-3.1.22 – Control Public Information 19

Level 2 AC Practices 21

AC.L2-3.1.3 – Control CUI Flow..... 21

AC.L2-3.1.4 – Separation of Duties..... 24

AC.L2-3.1.5 – Least Privilege..... 26

AC.L2-3.1.6 – Non-Privileged Account Use..... 28

AC.L2-3.1.7 – Privileged Functions 30

AC.L2-3.1.8 – Unsuccessful Logon Attempts 32

AC.L2-3.1.9 – Privacy & Security Notices..... 34

AC.L2-3.1.10 – Session Lock..... 36

AC.L2-3.1.11 – Session Termination 38
AC.L2-3.1.12 – Control Remote Access 40
AC.L2-3.1.13 – Remote Access Confidentiality 43
AC.L2-3.1.14 – Remote Access Routing 45
AC.L2-3.1.15 – Privileged Remote Access 47
AC.L2-3.1.16 – Wireless Access Authorization 49
AC.L2-3.1.17 – Wireless Access Protection 51
AC.L2-3.1.18 – Mobile Device Connection 54
AC.L2-3.1.19 – Encrypt CUI on Mobile 56
AC.L2-3.1.21 – Portable Storage Use 58

CMMC Assessment Guide

Level 2

Version 2.0 | December 2021

1. CMMC Assessment Guide (Level 2)
2. NIST Special Publication 800-171A
   Assessing Security Requirements for
   Controlled Unclassified Information
3. DoD Memo
   DoD Guidance for Reviewing System
   Security Plans and the NIST SP 800-
   171 Security Requirements

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

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].

Let's Look Closer

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

- ❑ Who Are The Authorized Users?
- ❑ Where Are They Identified?
- ❑ How Are They Authorized?

Let's Look Closer

[d] system access is limited to authorized users;

- ❑ What Authorizes Users onto the System?
- ❑ How Is Authorization Maintained/Reviewed?
- ❑ Can Authorization Be Removed/Granted At Will, By Whom, Process?

Control Requirements

Access Control Policies

- Acceptable Use Policy
- Account Authorization Form
- System Security Plan
- Onboard/Offboard Procedure

Technical Control/Management

- System Configuration
- Account Records
- Transaction Records

Record Keeping

- Authorization Records
- Account Management Reviews
- System Audit Logs
- Up to Date Account/Host Lists

3.1 Controls

Account Authorization	Permissions	Routing & Session Management	Configuration
3.1.1	3.1.4	3.1.3	3.1.8
3.1.2	3.1.5	3.1.11	3.1.9
3.1.15	3.1.6	3.1.12	3.1.10
3.1.16	3.1.7	3.1.13	3.1.17
3.1.18		3.1.14	3.1.19
3.1.22		3.1.20	3.1.21

Meeting the Controls

Process/Plan

- States Organization Intentions
- Defines Process
- Provides Path to Authorization

Implementation

- Shown through technical or non-technical process
- Can be observed
- Owner of this Control is defined

Enforcement

- Technical Restrictions In Place
- Consequences for Policy Breach Defined

Review

- Periodically Reviewed
- Review is Recorded
- This Review process is demonstrable
- Changes to process/control are subject to scrutiny

AC.L1-3.1.1 – AUTHORIZED ACCESS CONTROL

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

3.1.1 – Meeting the Controls

USER ACCOUNT AUTHORIZATION POLICY	**3.1.1[a] Authorized Users are Identified** **3.1.1[d] System is limited to authorized users.**
ACTIVE DIRECTORY	**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 processes acting on behalf of 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).**
HARDWARE/SOFTWARE INVENTORY NETWORK DIAGRAM	**3.1.1[c] Devices (and other systems) authorized to connect to system are identified.**

Permissions

3.1.4	**SECURITY REQUIREMENT** Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.4[a]	*the duties of individuals requiring separation are defined.*
	3.1.4[b]	*responsibilities for duties that require separation are assigned to separate individuals.*
	3.1.4[c]	*access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing divisions of responsibility and separation of duties; system security plan; system configuration settings and associated documentation; list of divisions of responsibility and separation of duties; system access authorizations; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with responsibilities for defining divisions of responsibility and separation of duties; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing separation of duties policy].	

3.1.4 – Meeting the Controls

ACCESS CONTROL POLICY

3.1.4[a] the duties of individuals requiring separation are defined.

3.1.4[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

ACTIVE DIRECTORY

3.1.4[b] responsibilities for duties that require separation are assigned to separate individuals.

3.1.4[c] access privileges that enable individuals to exercise the duties that require separation are granted to separate individuals.

Routing & Session Management

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 – Meeting the Controls

ACCESS CONTROL POLICY

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 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.

NETWORK DIAGRAM / BUSINESS PROCESS FLOW

3.1.3[b] methods and enforcement mechanisms for controlling the flow of CUI are defined.

3.1.3[c] designated sources and destinations for CUI within the system and between interconnected systems are identified.

Configuration

3.1.8	**SECURITY REQUIREMENT** Limit unsuccessful logon attempts.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.8[a] *the means of limiting unsuccessful logon attempts is defined.*
	3.1.8[b] *the defined means of limiting unsuccessful logon attempts is implemented.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; procedures addressing unsuccessful logon attempts; 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:* Personnel with information security responsibilities; system developers; system or network administrators]. Test: [*SELECT FROM:* Mechanisms implementing access control policy for unsuccessful logon attempts].

3.1.8 – Meeting the Controls

ACCESS CONTROL POLICY

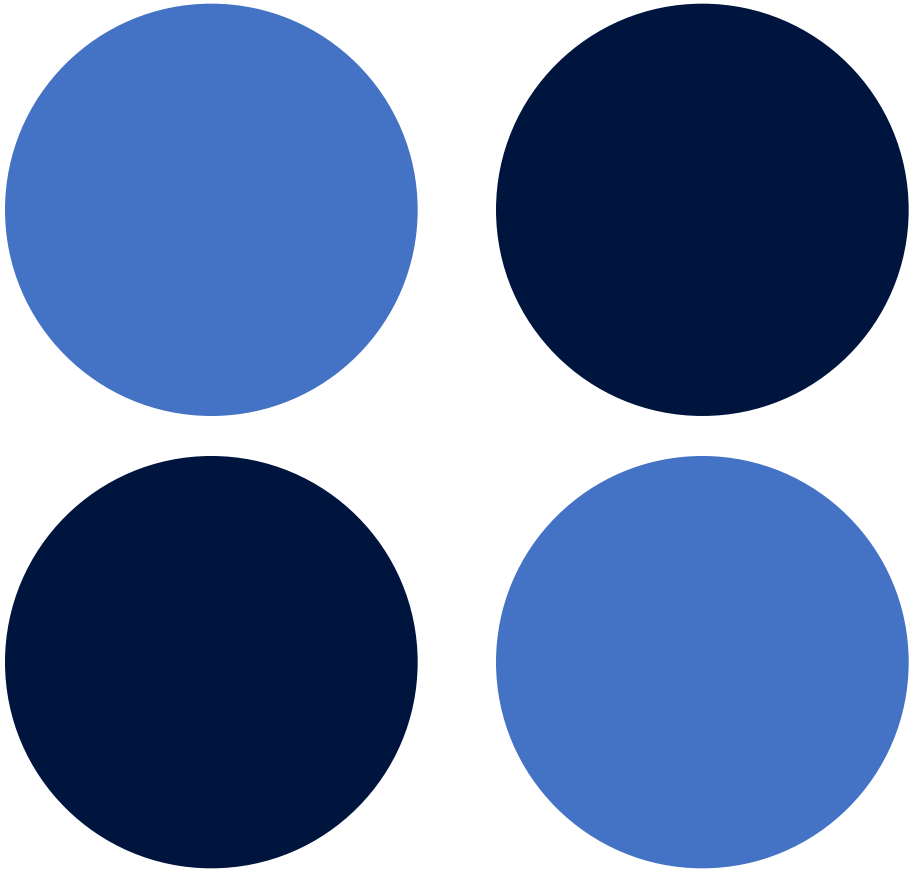
3.1.8[a] the means of limiting unsuccessful logon attempts is defined.

ACTIVE DIRECTORY

3.1.8[b] the defined means of limiting unsuccessful logon attempts is implemented.

Plan of Action and Milestones

Control Owners
are clearly defined.



Technical Control Artifacts
are collected, accurate, and available.

Processes
are documented and approved.

Reviews
are periodically conducted, tracked, and summarized.

Artifacts

Scoping Diagram

- Identifies Scoping Boundaries between CUI Assets, SPAs, CRMAs, Specialized Assets, and Out Of Scope Asssets

Network Diagram

- Identifies Interconnectivity Between Hardware and Cloud Resources within Assessment Environment

Inventories (Hardware/Software)

- Identifies Hardware, Software, and Cloud Assets within Assessment Environment

Policy Documentation

- States the Intention of the Architecture, Data Flow, and Restrictions on Usage within the Assessment Environment

Assessment Process

ASSESSMENT OBJECTIVES

Includes a determination statement related to the CUI security requirement that is the subject of the assessment.

Ex. 3.1.3 Control the flow of CUI in accordance with approved authorizations

ASSESSMENT METHODS

Define the nature and the extent of the assessor's actions. They include **examine**, **interview**, and **test**.

Ex. 3.1.3 Examine architectural solutions to control flow of system data.

ASSESSMENT OBJECTS

Identify specific items being assessed and can include specifications, mechanisms, activities, and individuals.

Ex. 3.1.3 Network Diagrams, Business Process Flow Diagrams

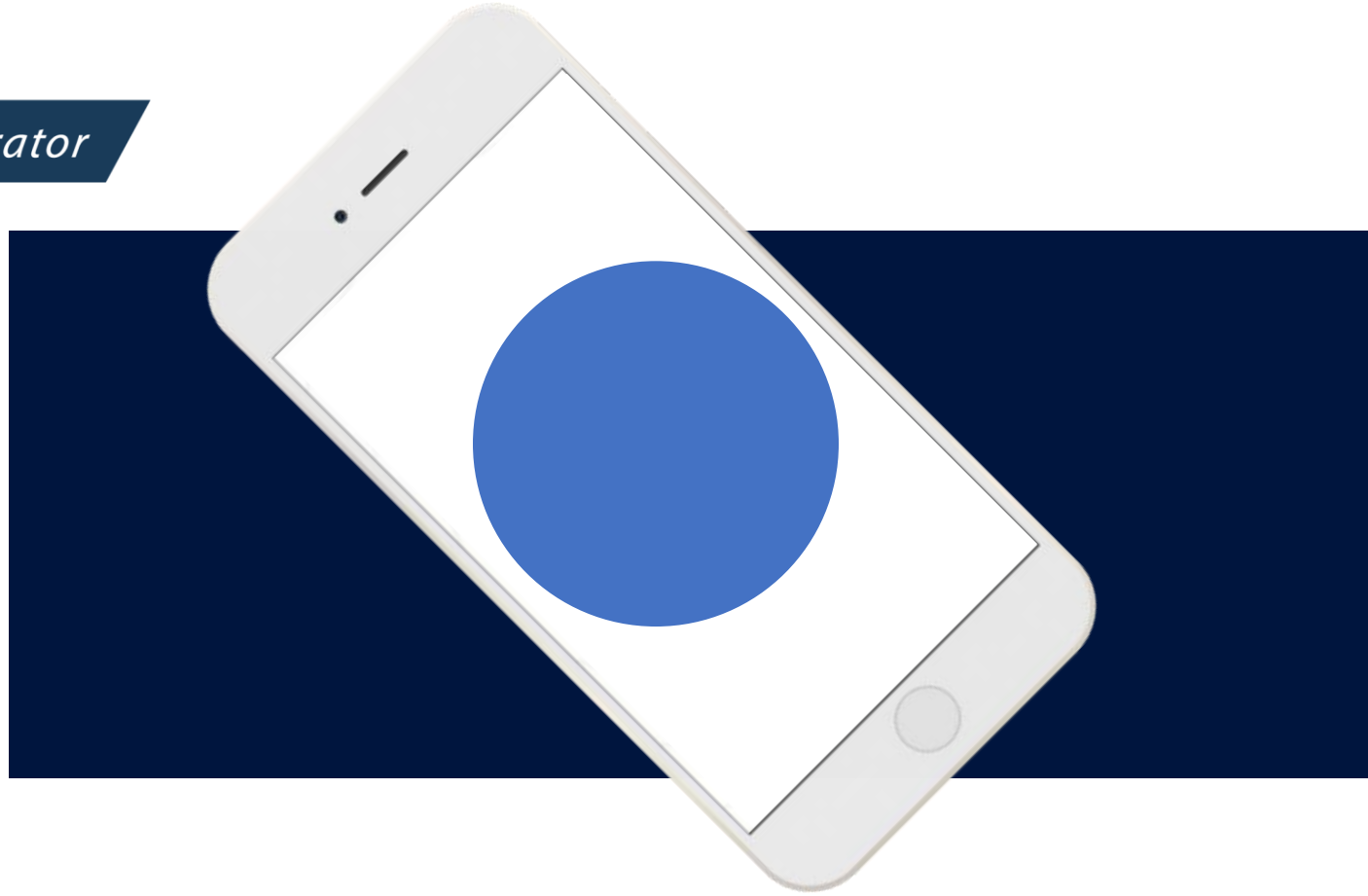
Assess each of the NIST SP 800-171 controls using the NIST SP 800-171A to ensure all audit points are covered.

Wisconsin Procurement Institute

An APEX Accelerator

Matthew Frost

mattf@wispro.org



APEX ACCELERATORS

Acquisition Hour

The Acquisition Hour webinar series covers a range of topics from market entry, sales growth, small business certifications, compliance, and more. Attendees receive 1 CPE credit for attending.

- **March 18** – Department of Defense Invoicing – PIEE / Wide Area Workflow
- **March 11** – An Introduction into the Supplier Performance Risk System (SPRS)

…More information and registrations at wispro.org/events

Cyber Thursday

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.

- **February 26** – CMMC: Control Set Series: 3.1 Access Control
- **March 26** – CMMC: Control Set Series: 3.2 Awareness and Training
- **April 30** – CMMC: Control Set Series: 3.3 Audit and Accountability
- **May 28** – CMMC: Control Set Series: 3.4 Configuration Management

…More information and registrations at wispro.org/events

Federal Market Insights

Federal Market Insights [FMI] is an informal podcast designed to provide valuable information about the government marketplace for businesses interested in government contracting.

- **March 17** – Government Property Programs
- **March 10** – Federal Contracts for Real Estate and Leasing Opportunities
- **March 3** – Issues Related to Debarment
- **February 24** – FAR 52.219-8 Utilization of Small Business Concern

…More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

February 26 2026

This webinar is eligible for

1 CPE credit

To receive a certificate of completion, contact apexaccelerator@wispro.org