Wisconsin Procurement Institute

An APEX Accelerator

Cyber Friday:

Building a CMMC Program: 3.1.4 Configuration Management Policy, Change Request Process, Baseline Configurations

August 23 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

Webinar Etiquette

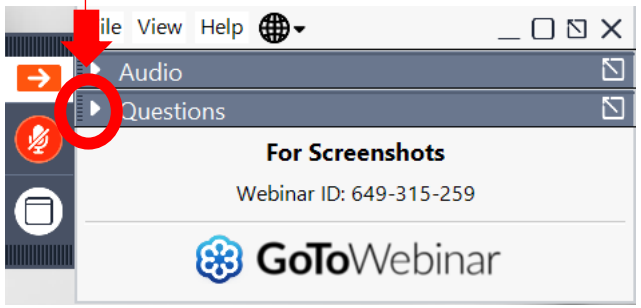
PLEASE

- 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!

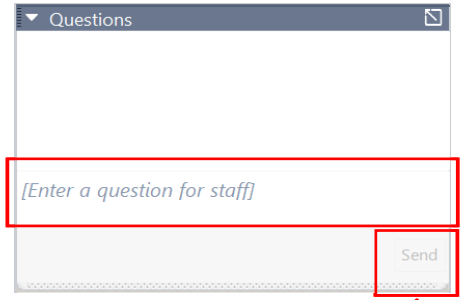
OPENING THE QUESTIONS BOX

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.

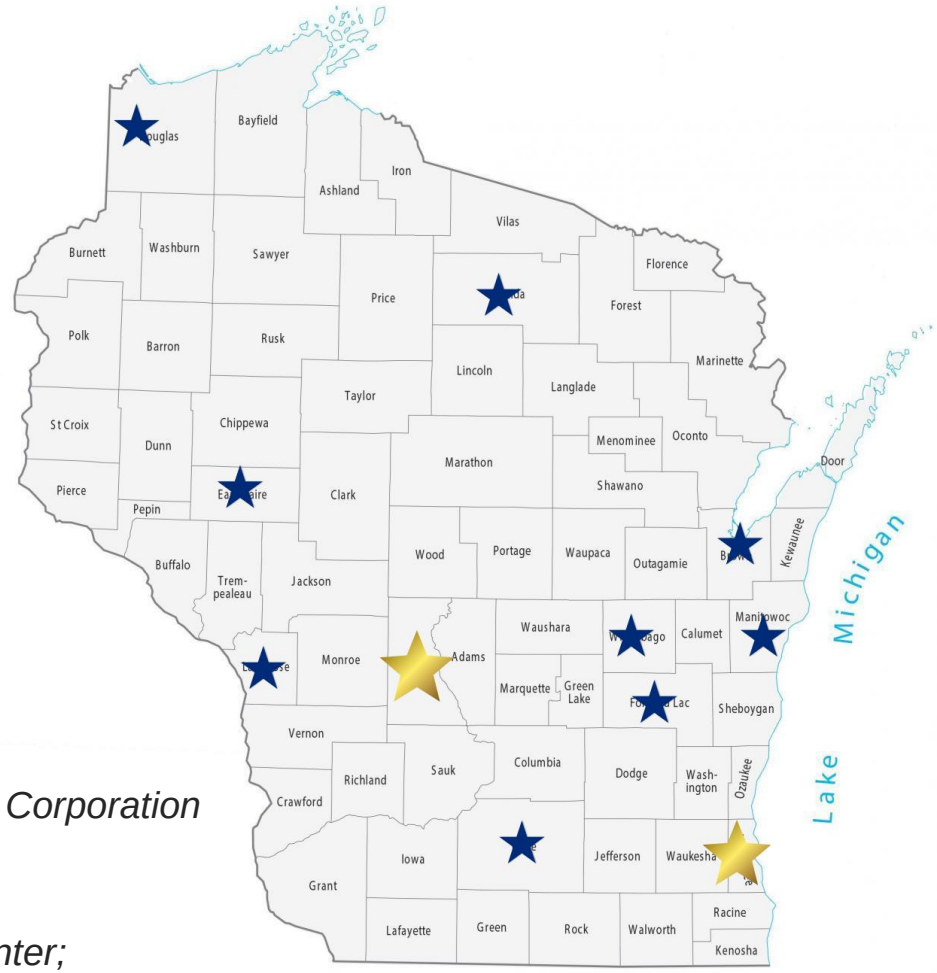
WPI provides services to all of Wisconsin's 72 counties

- 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……

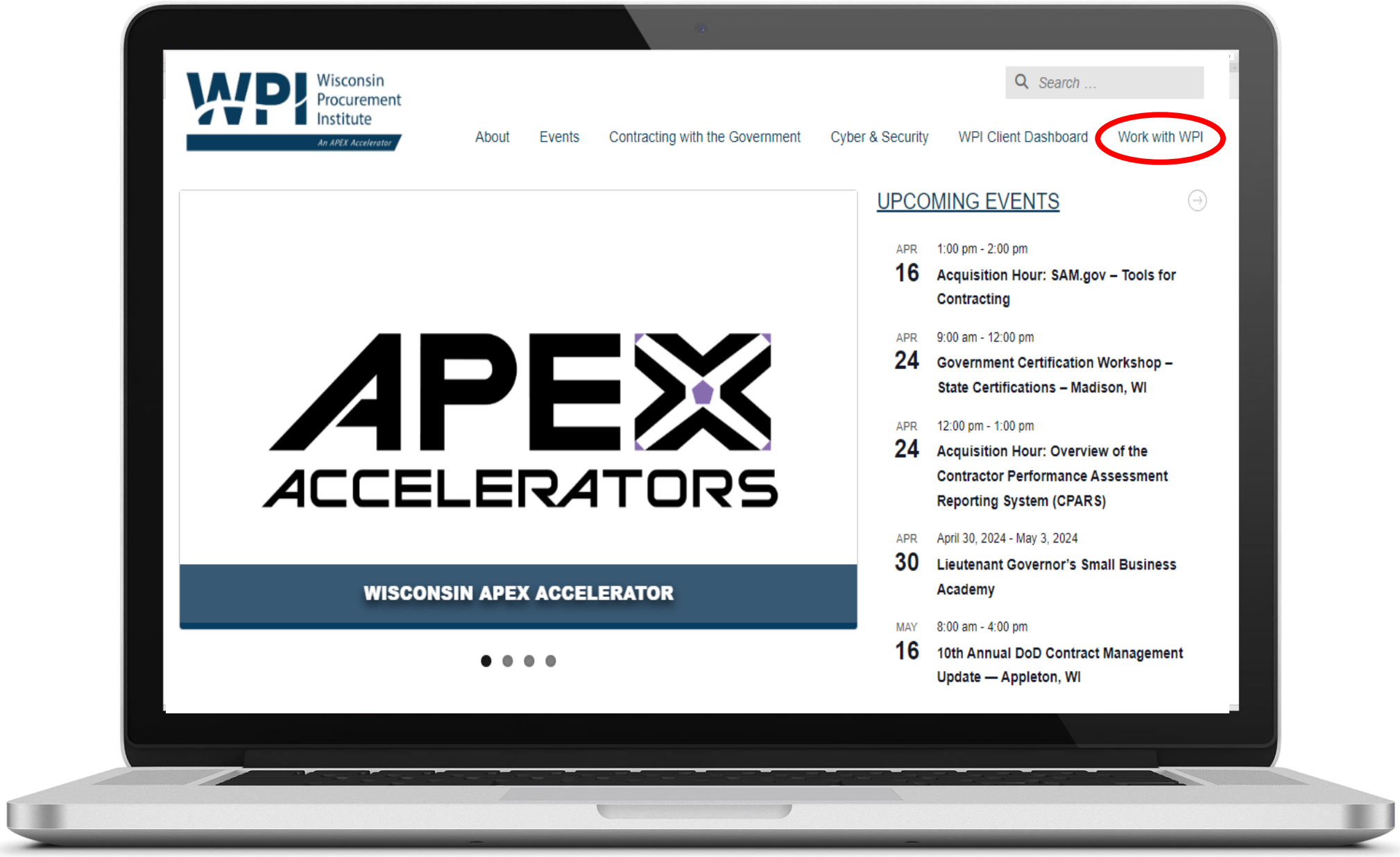
www.wispro.org

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*



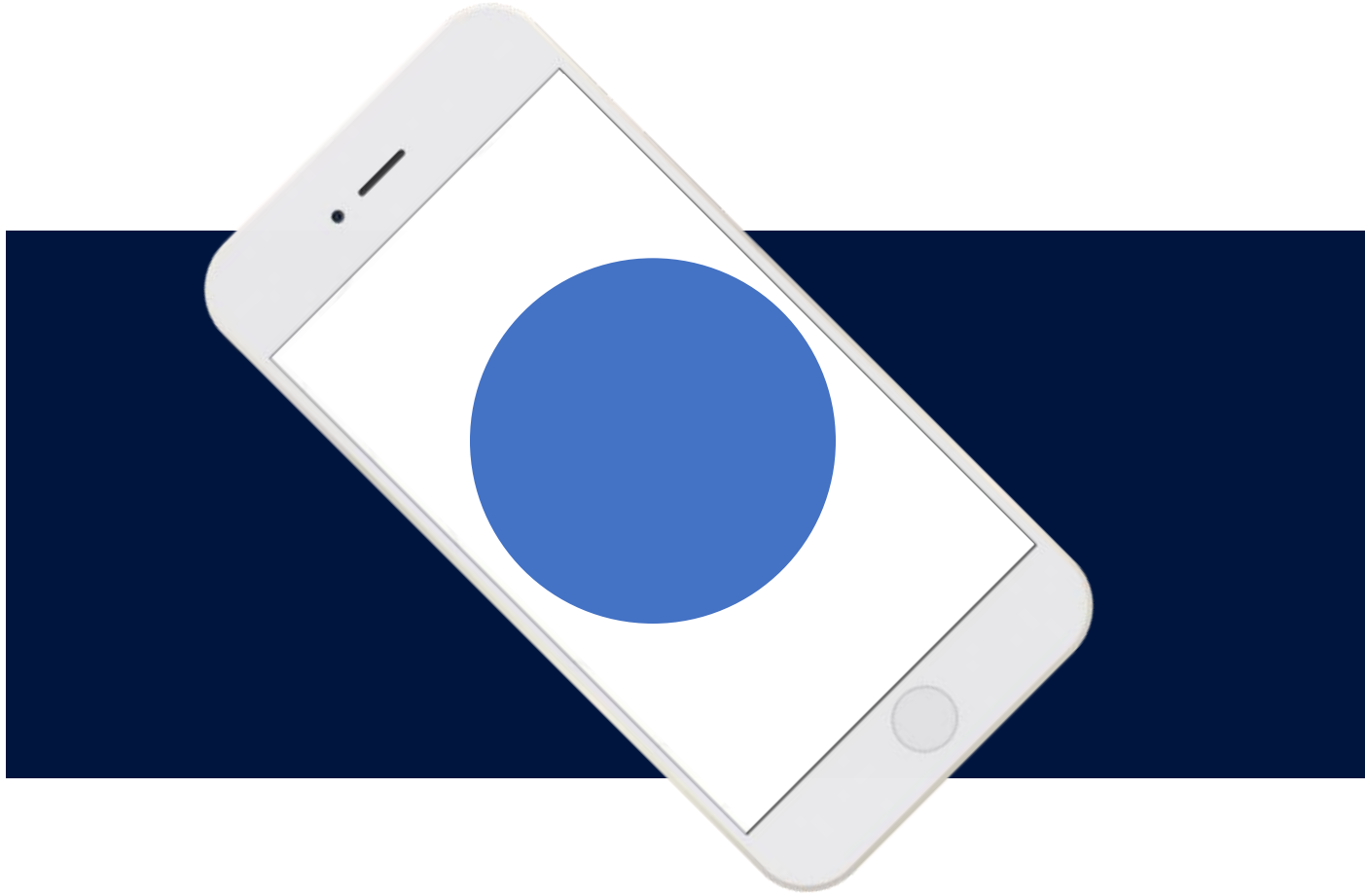
Wisconsin Procurement Institute
An APEX Accelerator


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 – July 19th, 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.

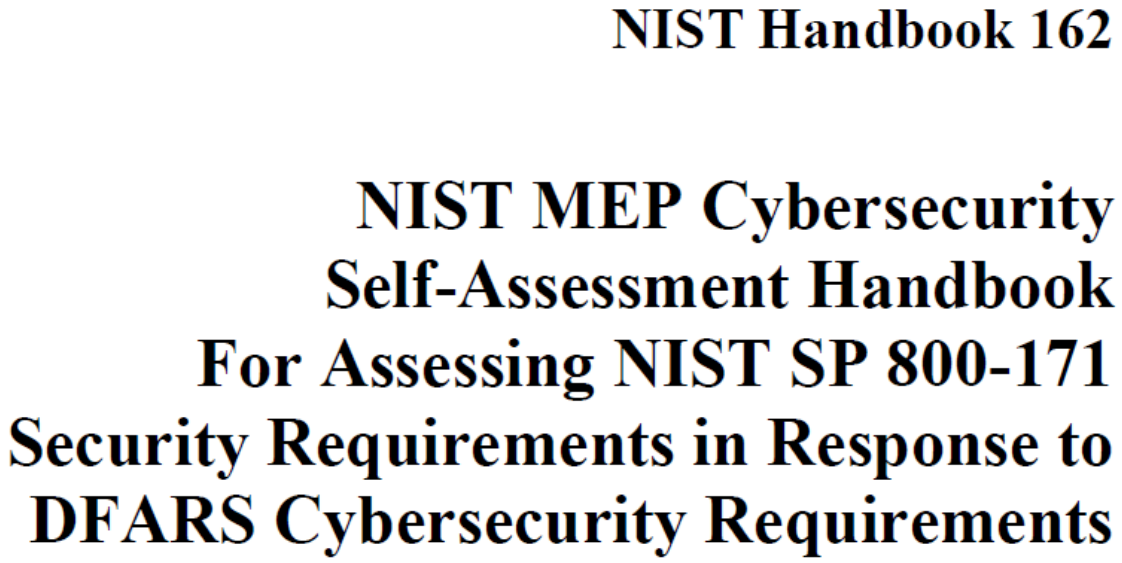
DFARS 252.204-7021

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 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

Configuration Management Policy

2

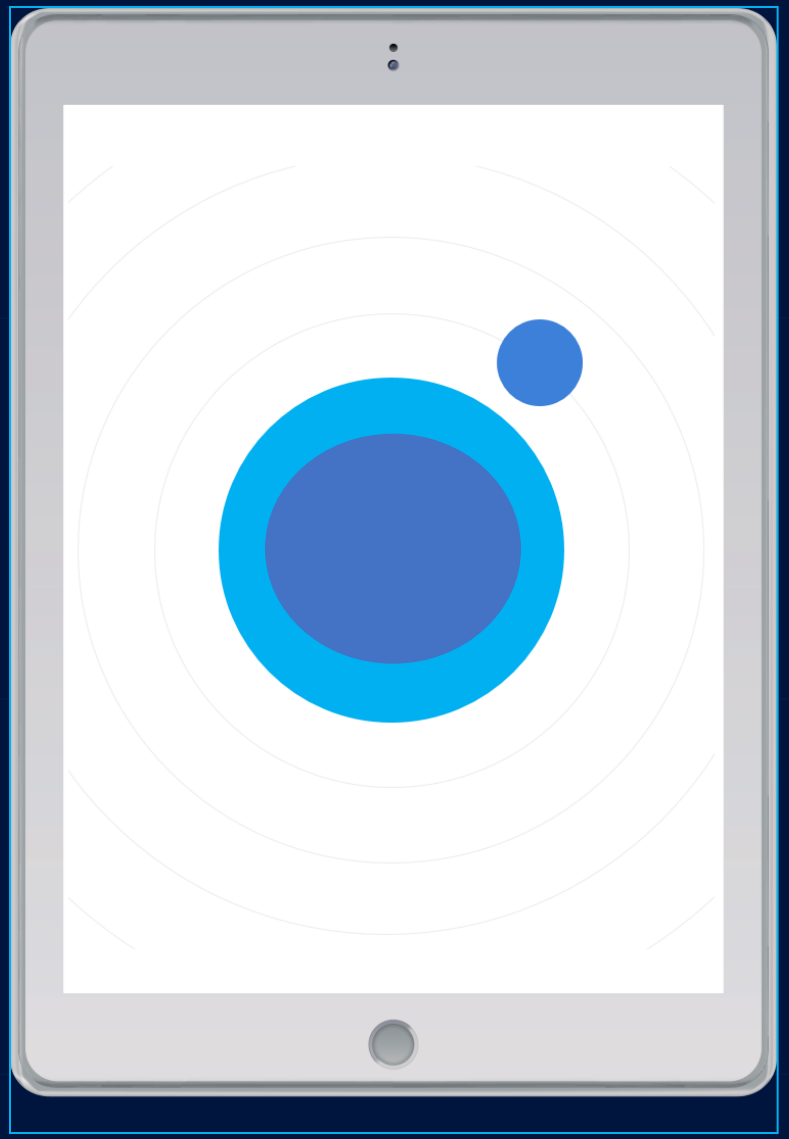
Network Diagram & Inventories

3

Change Request Form

Elements of the Policy

1. Purpose
2. Scope
3. Policy Statement
4. Definitions
    1. Baseline Configuration
    2. Configuration Item
5. Roles and Responsibilities process.
    1. Configuration Manager
    2. System/IT Administrators
    3. Change Control Board/Manager

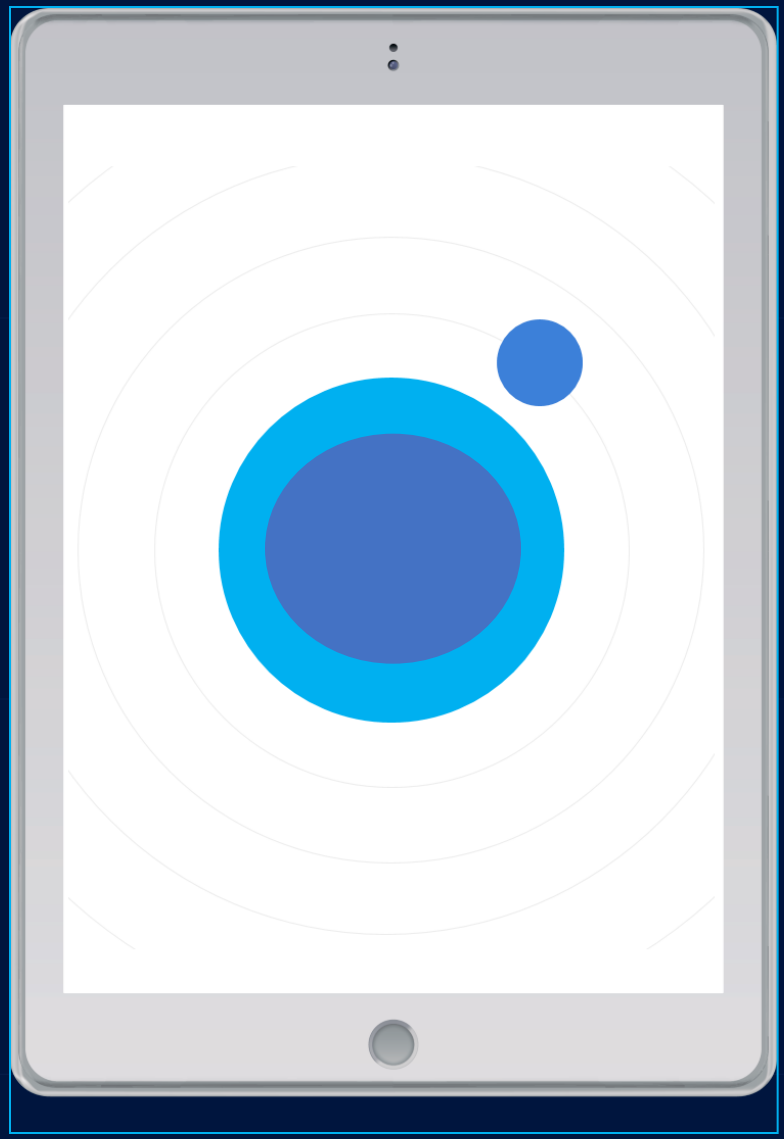


3.4.1	**SECURITY REQUIREMENT** Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.1[a] *a baseline configuration is established.*
	3.4.1[b] *the baseline configuration includes hardware, software, firmware, and documentation.*
	3.4.1[c] *the baseline configuration is maintained (reviewed and updated) throughout the system development life cycle.*
	3.4.1[d] *a system inventory is established.*
	3.4.1[e] *the system inventory includes hardware, software, firmware, and documentation.*
	3.4.1[f] *the inventory is maintained (reviewed and updated) throughout the system development life cycle.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Configuration management policy; procedures addressing the baseline configuration of the system; procedures addressing system inventory; system security plan; configuration management plan; system inventory records; inventory review and update records; enterprise architecture documentation; system design documentation; system architecture and configuration documentation; system configuration settings and associated documentation; change control records; system component installation records; system component removal records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with configuration management responsibilities; personnel with responsibilities for establishing the system inventory; personnel with responsibilities for updating the system inventory; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Organizational processes for managing baseline configurations; mechanisms supporting configuration control of the baseline configuration; organizational processes for developing and documenting an inventory of system components; organizational processes for updating inventory of system components; mechanisms supporting or implementing the system inventory; mechanisms implementing updating of the system inventory].

7. Baseline Configuration

- **General Workstation/Host Baseline**:
  - **Operating Systems**: Use only supported operating systems.
  - **Software Installation**: Only authorized software is allowed.
  - **Security Settings**:
    - Enable firewalls and configure according to organizational security policy.
    - Implement host-based intrusion detection/prevention systems.
    - Ensure antivirus and anti-malware solutions are installed and regularly updated.
    - Configure user access controls: implement least privilege and role-based access controls.
  - **Physical Security**: Lock down USB ports
  - **Network Configuration**:
    - Configure wired and wireless network settings
    - Disable unnecessary services and ports.
  - **Password Policies**:
  - **Encryption**:
  - **Audit Logging**:

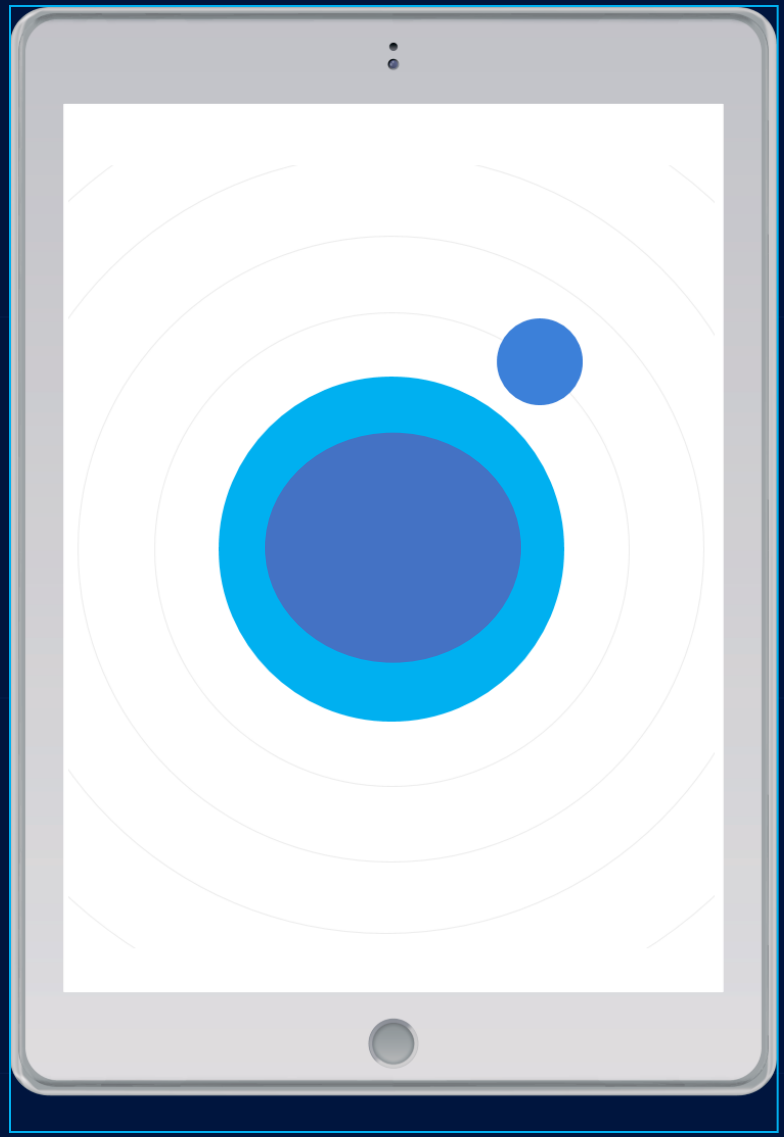
Elements of the Policy



3.4.2	**SECURITY REQUIREMENT** Establish and enforce security configuration settings for information technology products employed in organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.2[a]	*security configuration settings for information technology products employed in the system are established and included in the baseline configuration.*
	3.4.2[b]	*security configuration settings for information technology products employed in the system are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS	

Elements of the Policy

8. Configuration Control
9. Configuration Status Accounting
10. Configuration Audits
11. Security Configuration Management
12. Change Management
13. Training and Awareness
14. Compliance and Enforcement
15. Policy Review and Modification
16. Approval and Implementation
17. Appendices



Reading the Controls

NIST SP 800-171

1

Configuration Management Policy

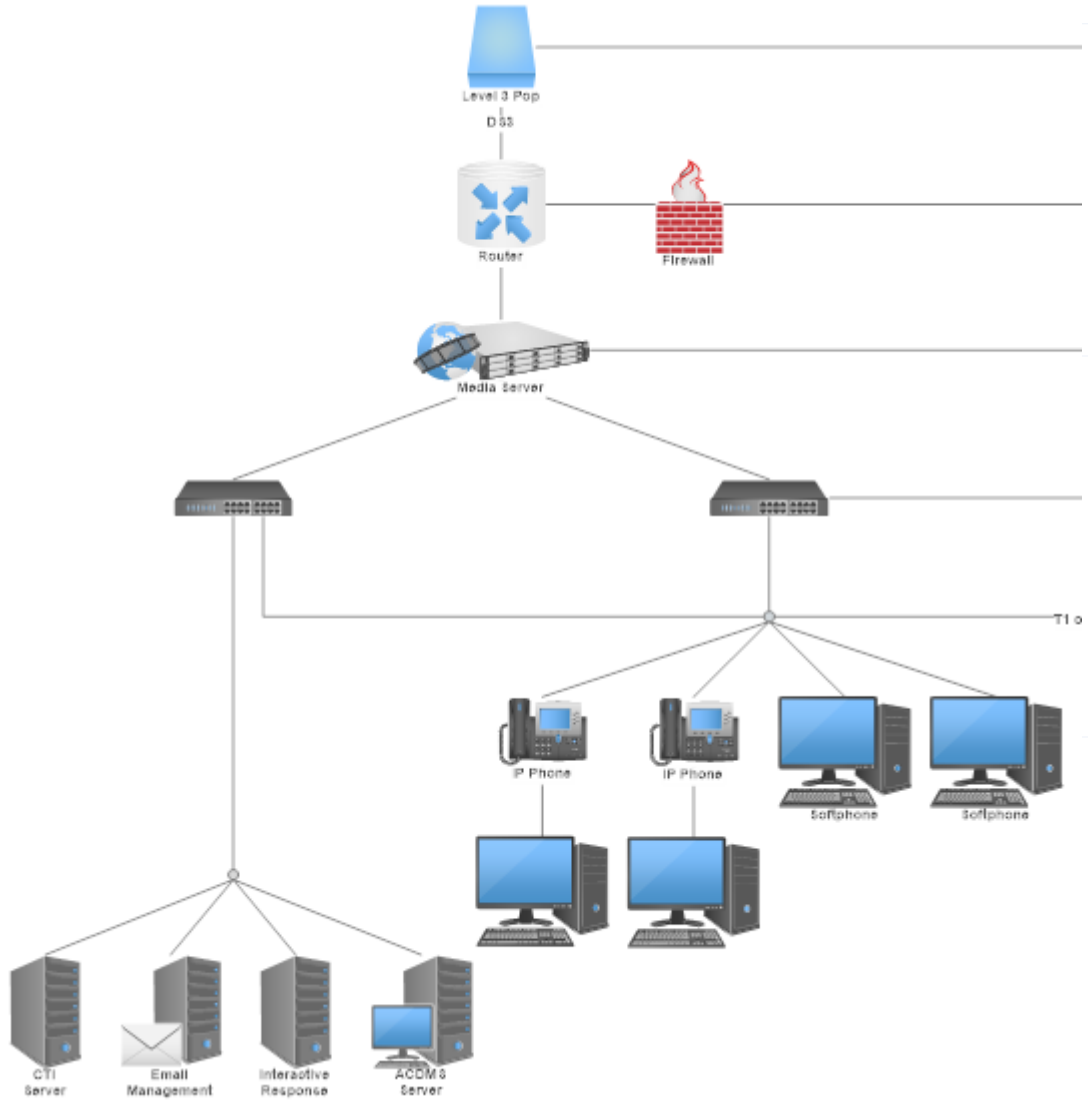
2

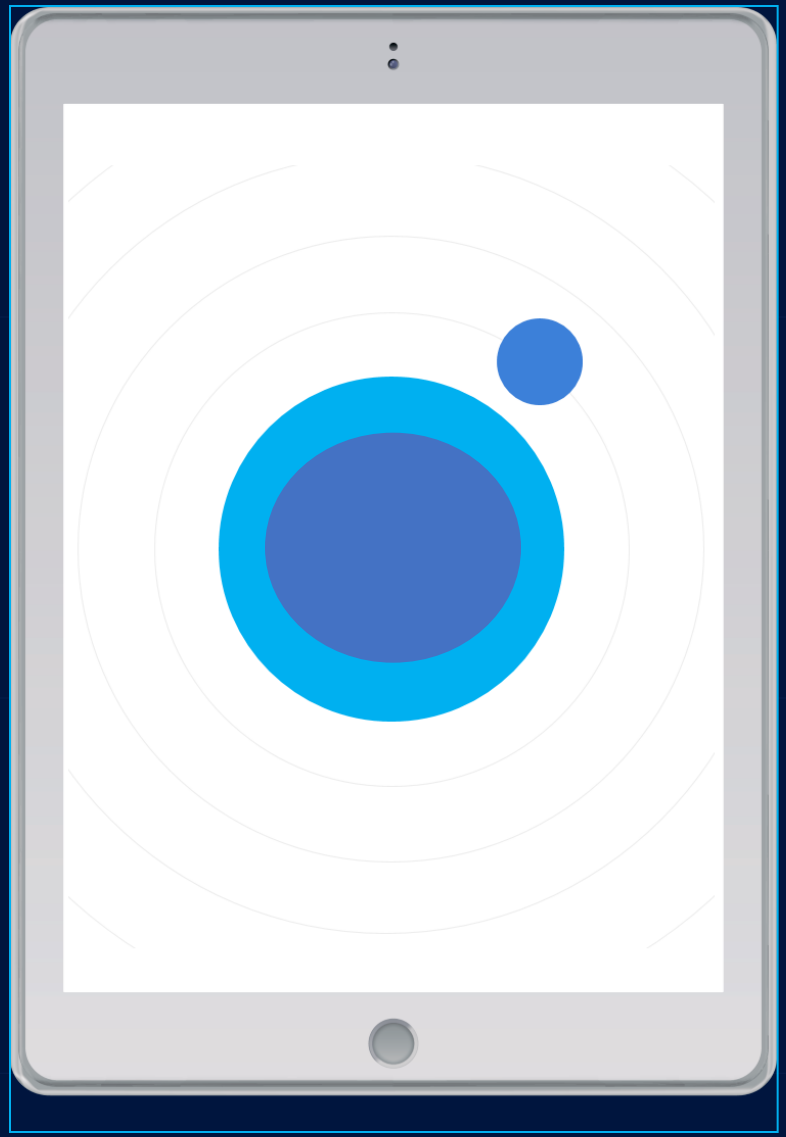
Network Diagram & Inventories

3

Change Request Form

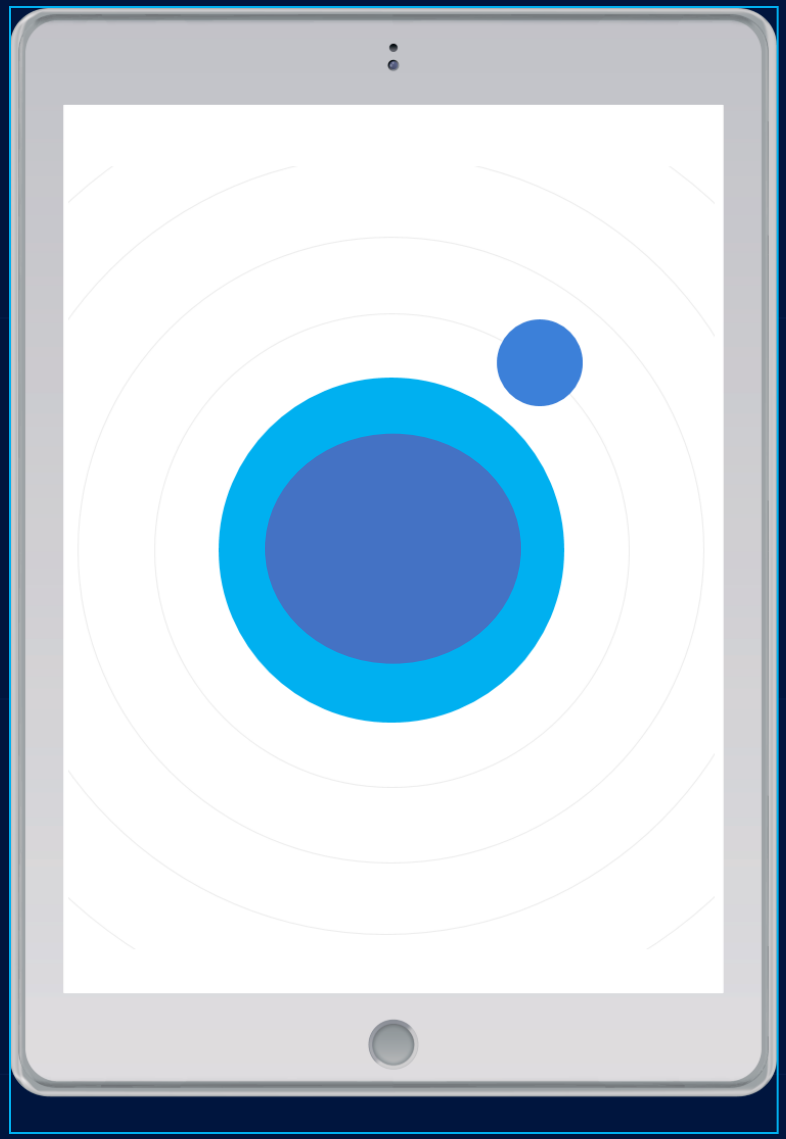
Network Diagram





1. **Secure Baseline Configurations (Control 3.4.1)**
2. **System Inventory Management (Control 3.4.2)**
3. **Effective Change Management (Control 3.4.9)**
4. **Security Configuration Monitoring and Compliance (Control 3.4.6)**
5. **Incident Response and Recovery (Controls 3.4.7 & 3.6.1)**
6. **System and Communications Protections (Control 3.13.5)**
7. **Documentation and Compliance Verification (Control 3.4.8)**

Network Diagram



3.4.9	**SECURITY REQUIREMENT** Control and monitor user-installed software.
	ASSESSMENT OBJECTIVE *Determine if:* 3.4.9[a] *a policy for controlling the installation of software by users is established.* 3.4.9[b] *installation of software by users is controlled based on the established policy.* 3.4.9[c] *installation of software by users is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Configuration management policy; procedures addressing user installed software; configuration management plan; system security plan; system design documentation; system configuration settings and associated documentation; list of rules governing user-installed software; system monitoring records; system audit logs and records; continuous monitoring strategy; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with responsibilities for governing user-installed software; personnel operating, using, or maintaining the system; personnel monitoring compliance with user-installed software policy; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Organizational processes governing user-installed software on the system; mechanisms enforcing rules or methods for governing the installation of software by users; mechanisms monitoring policy compliance].

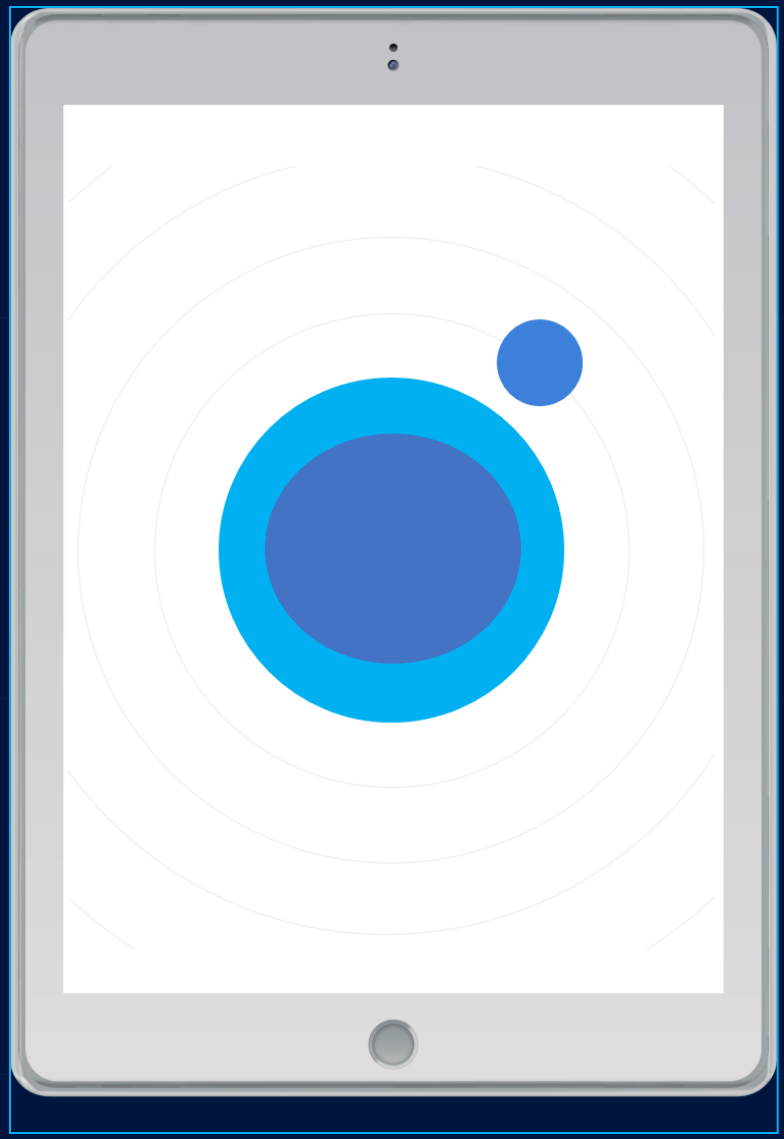
Software Installed in the Past 14 Days

Collection: Oxford Regional Office

Total number of computers: 7 Total number of titles: 18

Computer	User Name	Date	Publisher	Display Name	Version
CAOTTWHE-LEN	gartek\garth	20181015	Grammarly	Grammarly for Microsoft® Office Suite	6.7.141
CAOTTWHE-LEN	gartek\garth	20181018	Intel Corporation	Intel(R) Computing Improvement Program	2.4.04140
CAOTTWHE-LEN	gartek\garth	20181015	Mozilla	Mozilla Firefox 62.0.3 (x64 en-US)	62.0.3
CAOTTWHE-LEN	gartek\garth	20181017	Opera Software	Opera Stable 56.0.3051.43	56.0.3051.43
CM-CAS-CB1	gartek\cm16ssrs	20181022	Microsoft Corporation	Asset Intelligence Update Service Point	5.00.8692.1000
CM-CAS-CB1	gartek\cm16ssrs	20181019	Enhansoft	Enhansoft Reporting	6.045
CM-CAS-CB1	gartek\cm16ssrs	20181022	Enhansoft	Warranty Information Reporting v3.5	3.568
CM-PRI-CB2	n/a	20181022	Microsoft Corporation	Application Web Service	5.00.8692.1000
CM-PRI-CB2	n/a	20181022	Microsoft Corporation	BGB http proxy	5.00.8692.1000
CM-PRI-CB2	n/a	20181022	Microsoft Corporation	ConfigMgr Management Point	5.00.8692.1000
CM-PRI-CB2	n/a	20181022	Microsoft Corporation	Portal Web Site	5.00.8692.1000
ELLEN-PC	gartek\ellen	20181014	Adobe Systems Incorporated	Adobe Flash Player 31 ActiveX	31.0.0.122
ES-06	gartek\garth	20181023	Adobe Systems Incorporated	Adobe Acrobat Reader DC	19.008.20080
ES-06	gartek\garth	20181022	Microsoft Corporation	Microsoft .NET Framework 4.5.2	4.5.51209
ES-06	gartek\garth	20181022	Microsoft Corporation	Security Update for Microsoft .NET Framework 4.5.2 (KB4338602)	1
ST3	gartek\stighe	20181011	Adobe Systems Incorporated	Adobe Flash Player 31 NPAPI	31.0.0.122
ST3	gartek\stighe	20181022	The GIMP Team	GIMP 2.10.6	2.10.6
WIRE3	gartek\garth	20181019	Google, Inc.	Google Chrome	70.0.3538.67

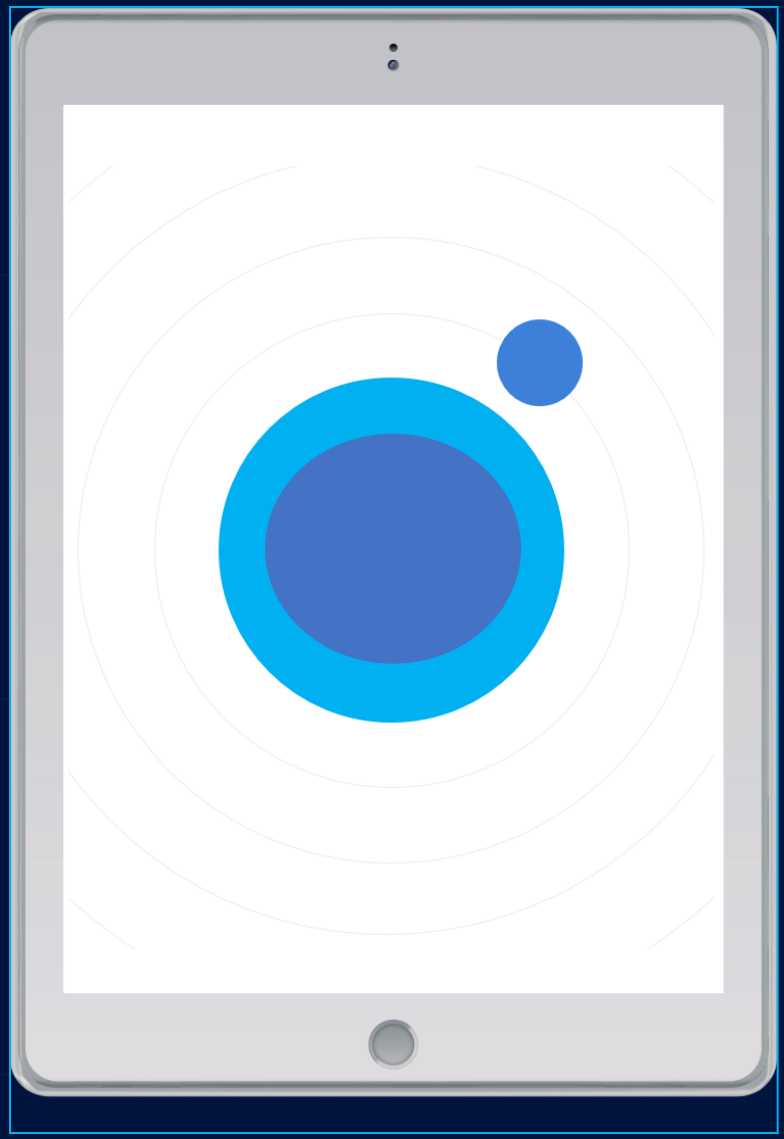
Inventories



3.4.7	SECURITY REQUIREMENT Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.7[a]	*essential programs are defined.*
	3.4.7[b]	*the use of nonessential programs is defined.*
	3.4.7[c]	*the use of nonessential programs is restricted, disabled, or prevented as defined.*
	3.4.7[d]	*essential functions are defined.*
	3.4.7[e]	*the use of nonessential functions is defined.*
	3.4.7[f]	*the use of nonessential functions is restricted, disabled, or prevented as defined.*
	3.4.7[g]	*essential ports are defined.*
	3.4.7[h]	*the use of nonessential ports is defined.*
	3.4.7[i]	*the use of nonessential ports is restricted, disabled, or prevented as defined.*
	3.4.7[j]	*essential protocols are defined.*
	3.4.7[k]	*the use of nonessential protocols is defined.*
	3.4.7[l]	*the use of nonessential protocols is restricted, disabled, or prevented as defined.*
	3.4.7[m]	*essential services are defined.*
	3.4.7[n]	*the use of nonessential services is defined.*
	3.4.7[o]	*the use of nonessential services is restricted, disabled, or prevented as defined.*

Protocol and Port	Type of traffic	AD and AD DS Usage
TCP and UDP 389	LDAP	Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP 636	LDAP SSL	Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP 3268	LDAP GC	Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP 3269	LDAP GC SSL	Directory, Replication, User and Computer Authentication, Group Policy, Trusts
TCP and UDP 88	Kerberos	User and Computer Authentication, Forest Level Trusts
TCP and UDP 53	DNS	User and Computer Authentication, Name Resolution, Trusts
TCP and UDP 445	SMB,CIFS,SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc	Replication, User and Computer Authentication, Group Policy, Trusts
TCP 25	SMTP	Replication
TCP 135	RPC, EPM	Replication
TCP Dynamic	RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS	Replication, User and Computer Authentication, Group Policy, Trusts
TCP 5722	RPC, DFSR (SYSVOL)	File Replication
UDP 123	Windows Time	Windows Time, Trusts
TCP and UDP 464	Kerberos change/set password	Replication, User and Computer Authentication, Trusts
UDP Dynamic	DCOM, RPC, EPM	Group Policy
UDP 138	DFSN, NetLogon, NetBIOS Datagram Service	DFS, Group Policy
TCP 9389	SOAP	AD DS Web Services
UDP 67 and UDP 2535	DHCP, MADCAP	DHCP
UDP 137	NetLogon, NetBIOS Name Resolution	User and Computer Authentication,
TCP 139	DFSN, NetBIOS Session Service, NetLogon	User and Computer Authentication, Replication

Access Control List



Reading the Controls

NIST SP 800-171

1

Configuration Management Policy

2

Network Diagram & Inventories

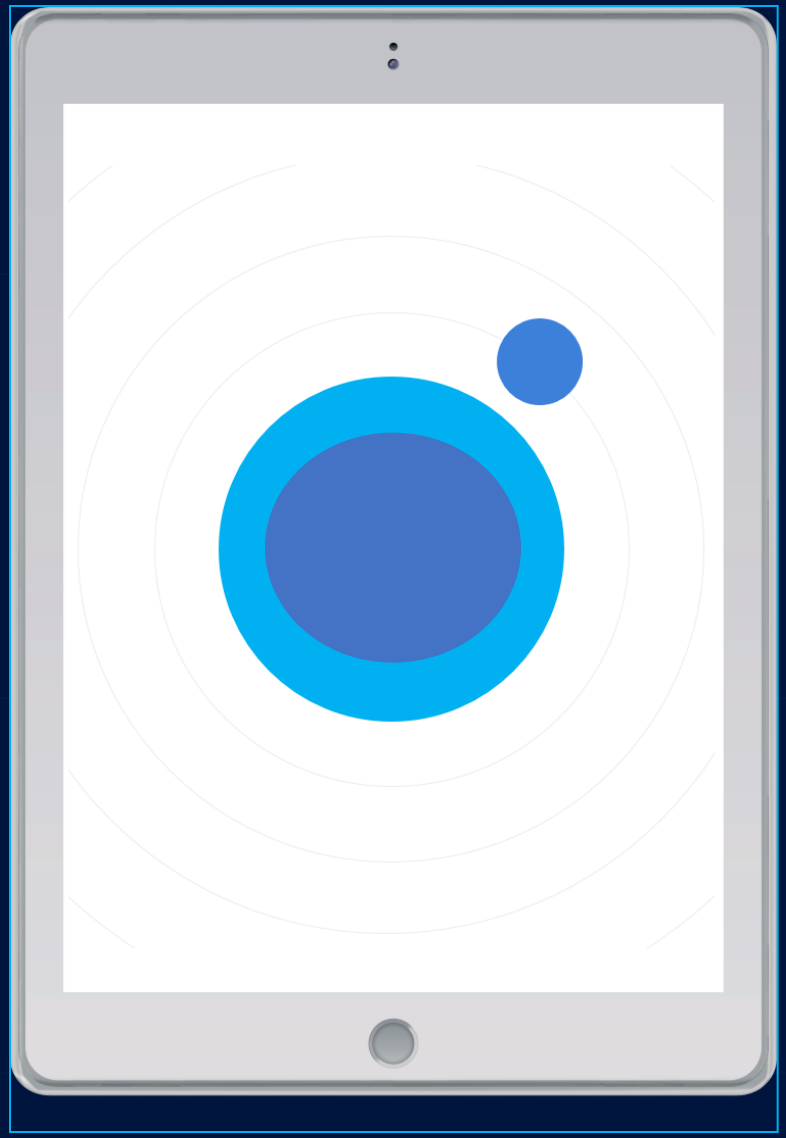
3

Change Request Form

Change Request Form Template

Project Name	Name of project		
Requested By	Name of requestor	Date	Date request was raised
Request No	Request Number	Name of Request	Brief name of request
Change Description	Description of the change		
Change Reason	Give the justification for the change		
Impact of change	Specify the impact of the change in terms of cost impact, budget impact, schedule impact, and impact on other projects.		
Proposed Action	Does the project manager propose this change is accepted/rejected and why		
Status	In review	Approved	Rejected
Approval Date	The date the change was approved or rejected		
Approved By	Who approved the change (usually the project manager or project sponsor)		

Change Request Form



3.4.3	SECURITY REQUIREMENT Track, review, approve or disapprove, and log changes to organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:* 3.4.3[a] *changes to the system are tracked.* 3.4.3[b] *changes to the system are reviewed.* 3.4.3[c] *changes to the system are approved or disapproved.* 3.4.3[d] *changes to the system are logged.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Configuration management policy; procedures addressing system configuration change control; configuration management plan; system architecture and configuration documentation; system security plan; change control records; system audit logs and records; change control audit and review reports; agenda/minutes from configuration change control oversight meetings; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with configuration change control responsibilities; personnel with information security responsibilities; system or network administrators; members of change control board or similar]. Test: [*SELECT FROM:* Organizational processes for configuration change control; mechanisms that implement configuration change control].

3.4.4	**SECURITY REQUIREMENT** Analyze the security impact of changes prior to implementation.
	ASSESSMENT OBJECTIVE *Determine if the security impact of changes to the system is analyzed prior to implementation.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Configuration management policy; procedures addressing security impact analysis for system changes; configuration management plan; security impact analysis documentation; system security plan; analysis tools and associated outputs; change control records; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with responsibility for conducting security impact analysis; personnel with information security responsibilities; system or network administrators]. Test: [*SELECT FROM:* Organizational processes for security impact analysis].

3.4.5	SECURITY REQUIREMENT Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.5[a]	*physical access restrictions associated with changes to the system are defined.*
	3.4.5[b]	*physical access restrictions associated with changes to the system are documented.*
	3.4.5[c]	*physical access restrictions associated with changes to the system are approved.*
	3.4.5[d]	*physical access restrictions associated with changes to the system are enforced.*
	3.4.5[e]	*logical access restrictions associated with changes to the system are defined.*
	3.4.5[f]	*logical access restrictions associated with changes to the system are documented.*
	3.4.5[g]	*logical access restrictions associated with changes to the system are approved.*
	3.4.5[h]	*logical access restrictions associated with changes to the system are enforced.*

3.4.6	**SECURITY REQUIREMENT** Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.4.6[a] *essential system capabilities are defined based on the principle of least functionality.*
	3.4.6[b] *the system is configured to provide only the defined essential capabilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Configuration management policy; configuration management plan; procedures addressing least functionality in the system; system security plan; system design documentation; system configuration settings and associated documentation; security configuration checklists; other relevant documents or records].

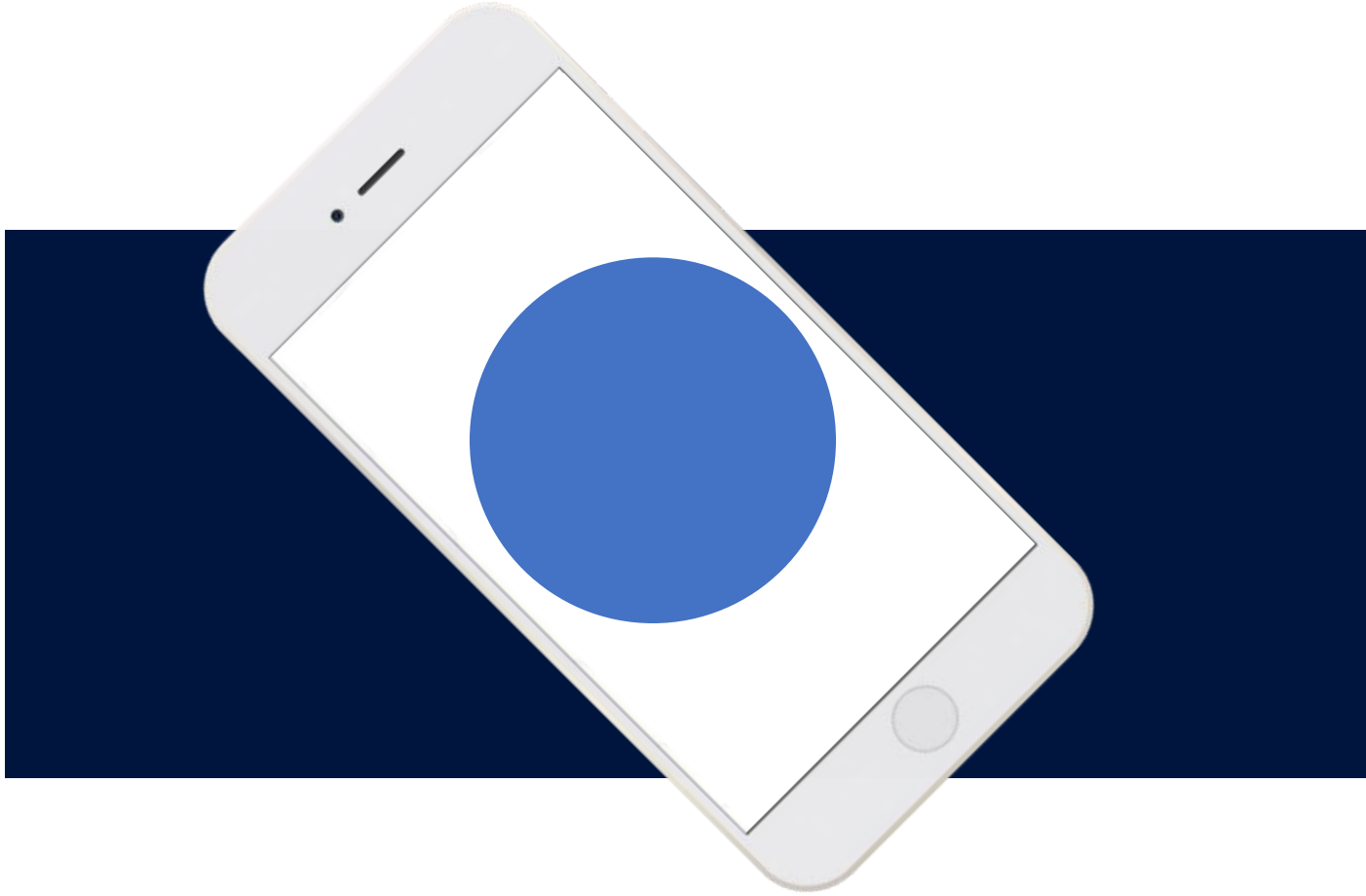
3.4.7	SECURITY REQUIREMENT Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.4.7[a]	*essential programs are defined.*
	3.4.7[b]	*the use of nonessential programs is defined.*
	3.4.7[c]	*the use of nonessential programs is restricted, disabled, or prevented as defined.*
	3.4.7[d]	*essential functions are defined.*
	3.4.7[e]	*the use of nonessential functions is defined.*
	3.4.7[f]	*the use of nonessential functions is restricted, disabled, or prevented as defined.*
	3.4.7[g]	*essential ports are defined.*
	3.4.7[h]	*the use of nonessential ports is defined.*
	3.4.7[i]	*the use of nonessential ports is restricted, disabled, or prevented as defined.*
	3.4.7[j]	*essential protocols are defined.*
	3.4.7[k]	*the use of nonessential protocols is defined.*
	3.4.7[l]	*the use of nonessential protocols is restricted, disabled, or prevented as defined.*
	3.4.7[m]	*essential services are defined.*
	3.4.7[n]	*the use of nonessential services is defined.*
	3.4.7[o]	*the use of nonessential services is restricted, disabled, or prevented as defined.*

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

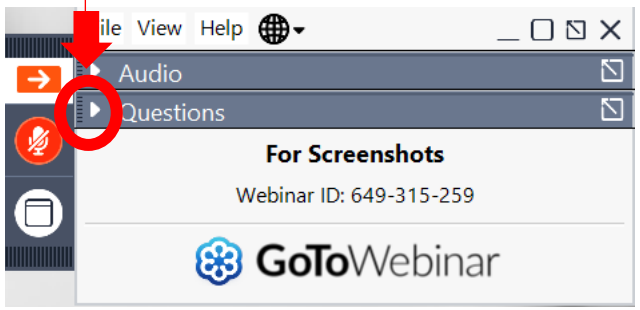
AN APEX ACCELERATOR



QUESTIONS?

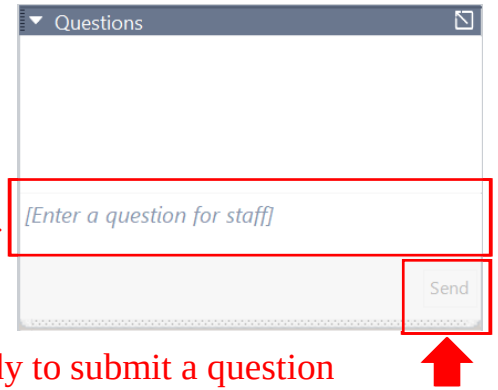
OPENING THE QUESTIONS BOX

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.

- **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

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.

- ~~**July 25 –** Beyond contracts: Conducting Business with the Federal Government~~
- ~~**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

WPI 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

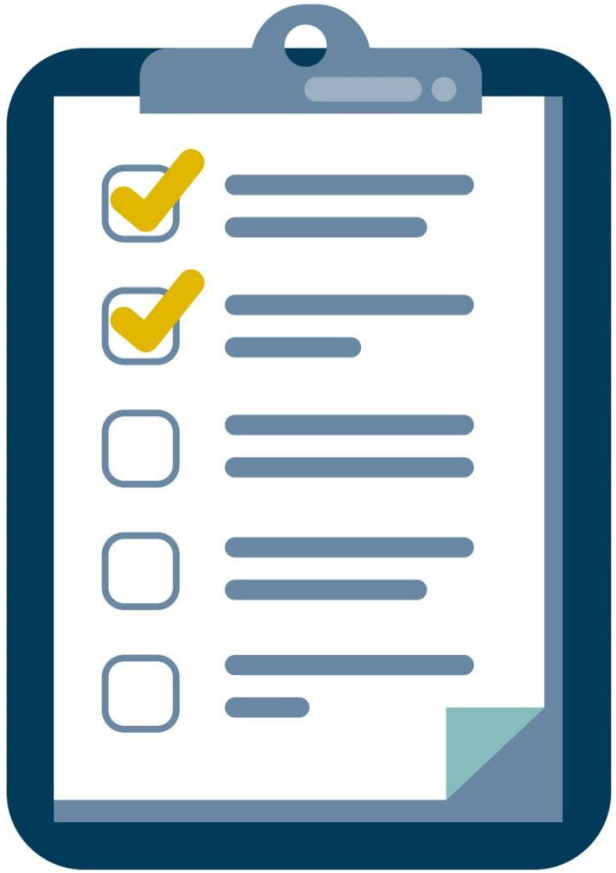
The Contracting Academy (TCA) is an opportunity for businesses to grow their technical knowledge of contracting with Federal Government, State/Local Government, and Government Prime Contractors. The series of workshops will benefit established businesses looking to grow and develop their government sales.

…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

August 23, 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