Cyber Friday:

CMMC: Maintaining Your CMMC Certification

April 25 | 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.

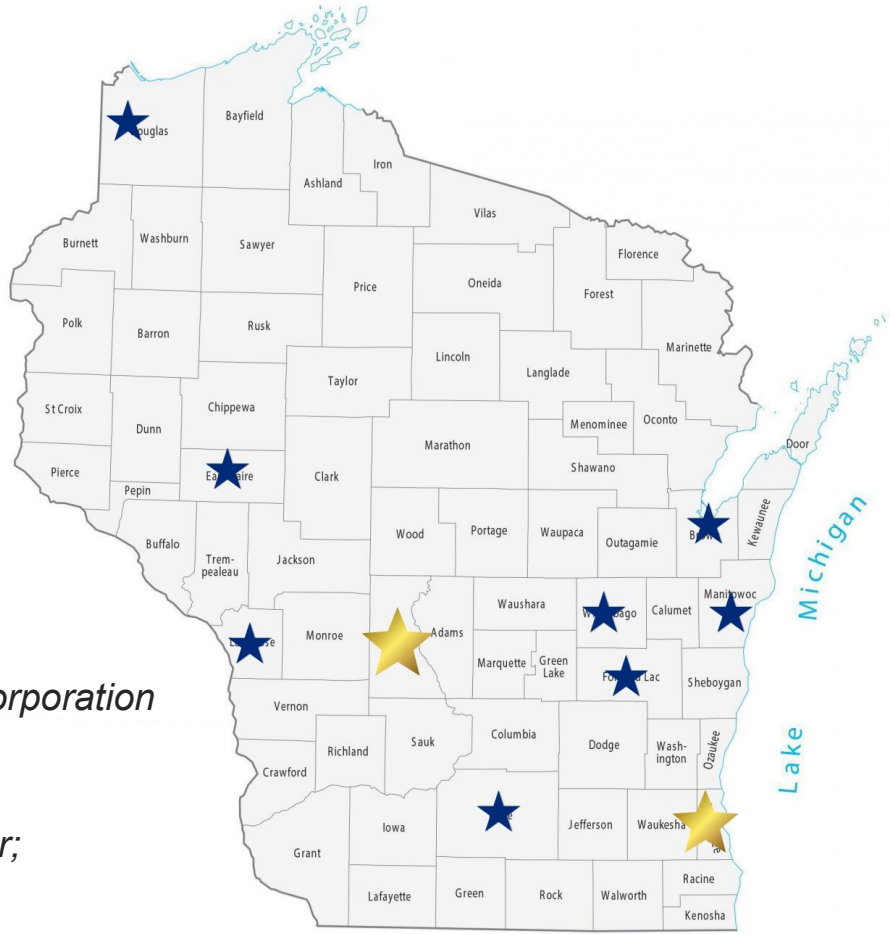
WPI provides services and training to all of Wisconsin's 72 counties

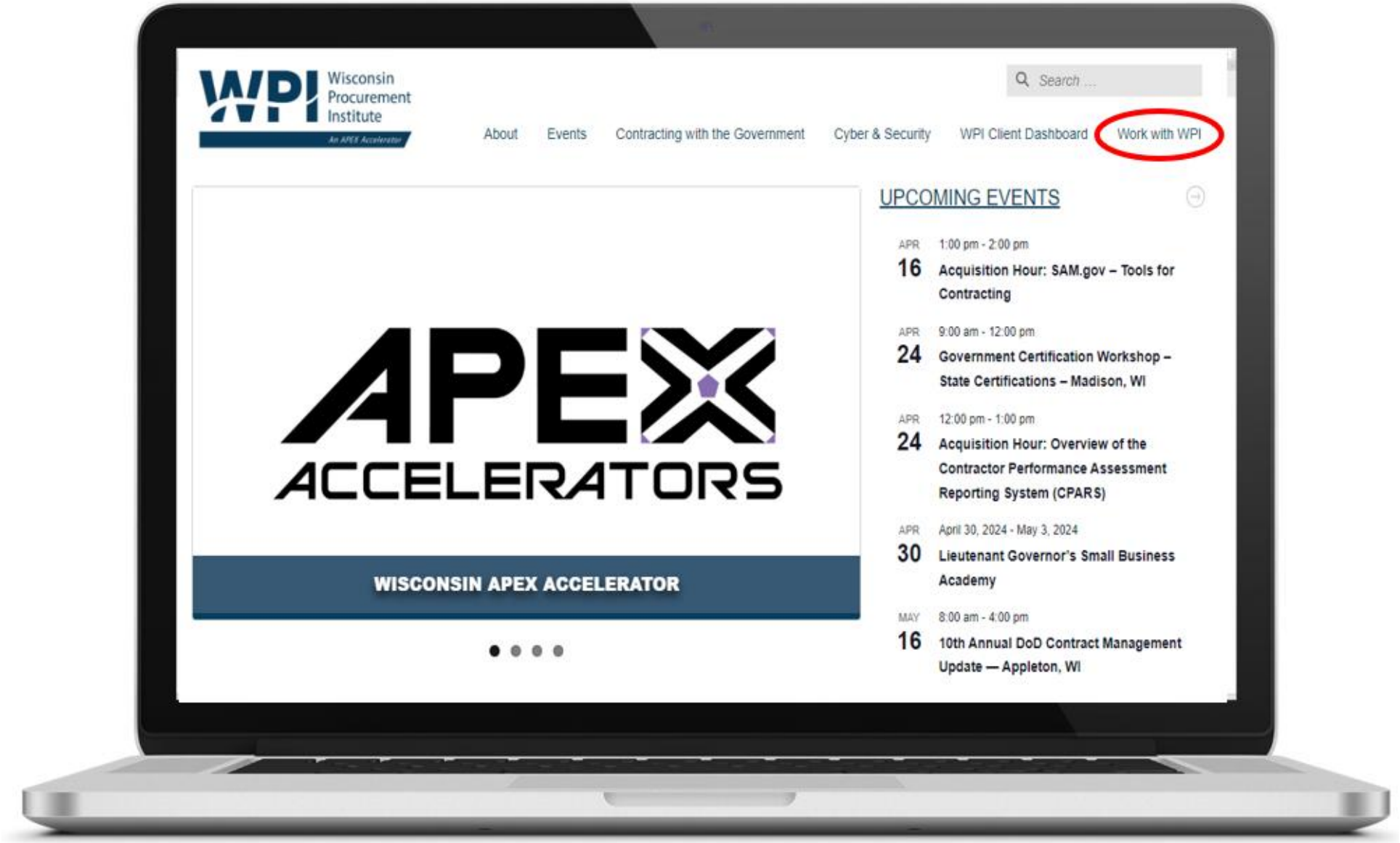
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting 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*
  - *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*

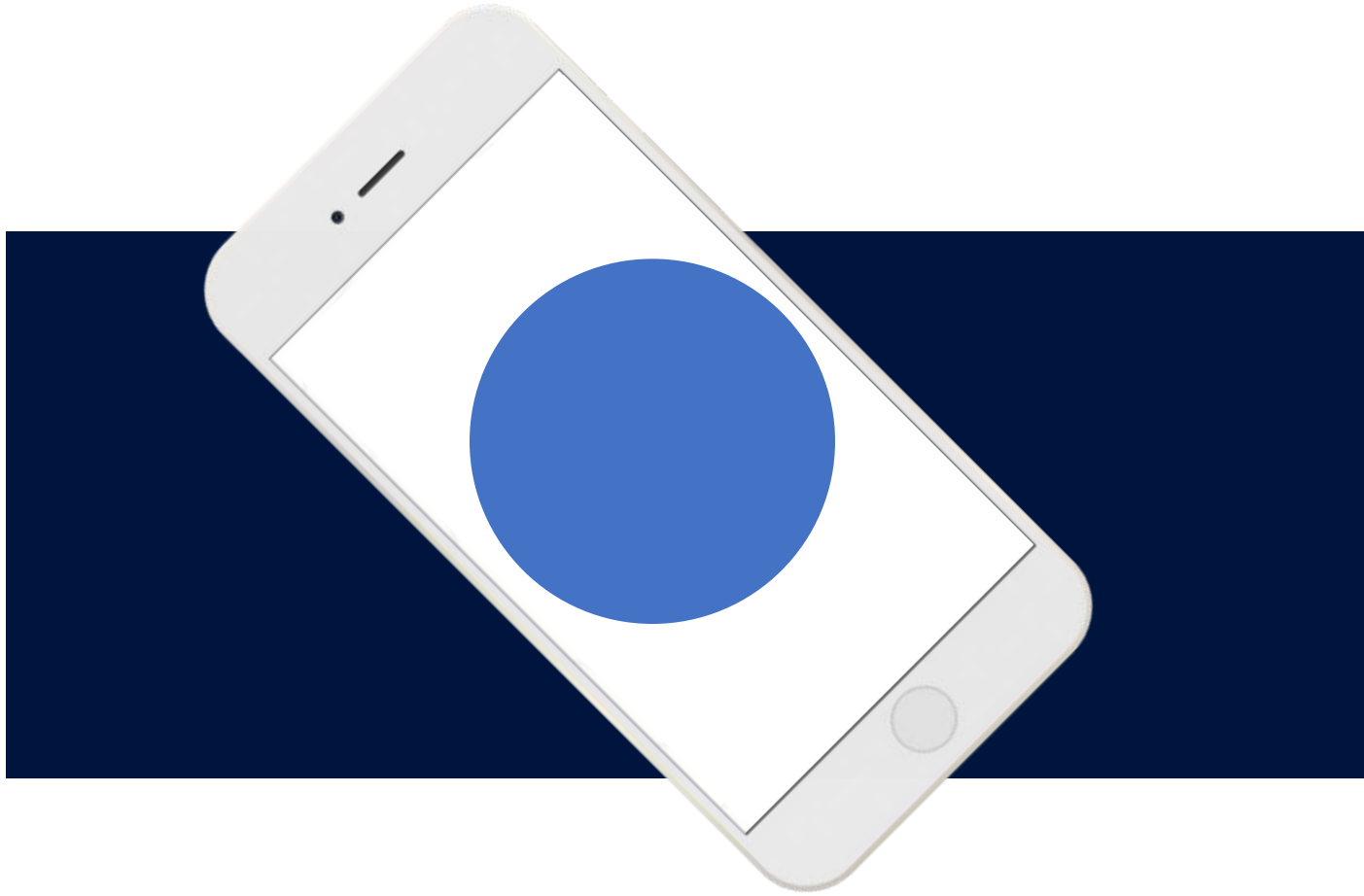



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR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

CMMC: Maintaining Your CMMC Certification

Wisconsin Procurement Institute

An APEX Accelerator



CYBER FRIDAY SESSIONS – April 25th, 2025

Confirmed in 2013, the theft of data from the F-35 Lightning II represented one of the most significant data breaches in world history.

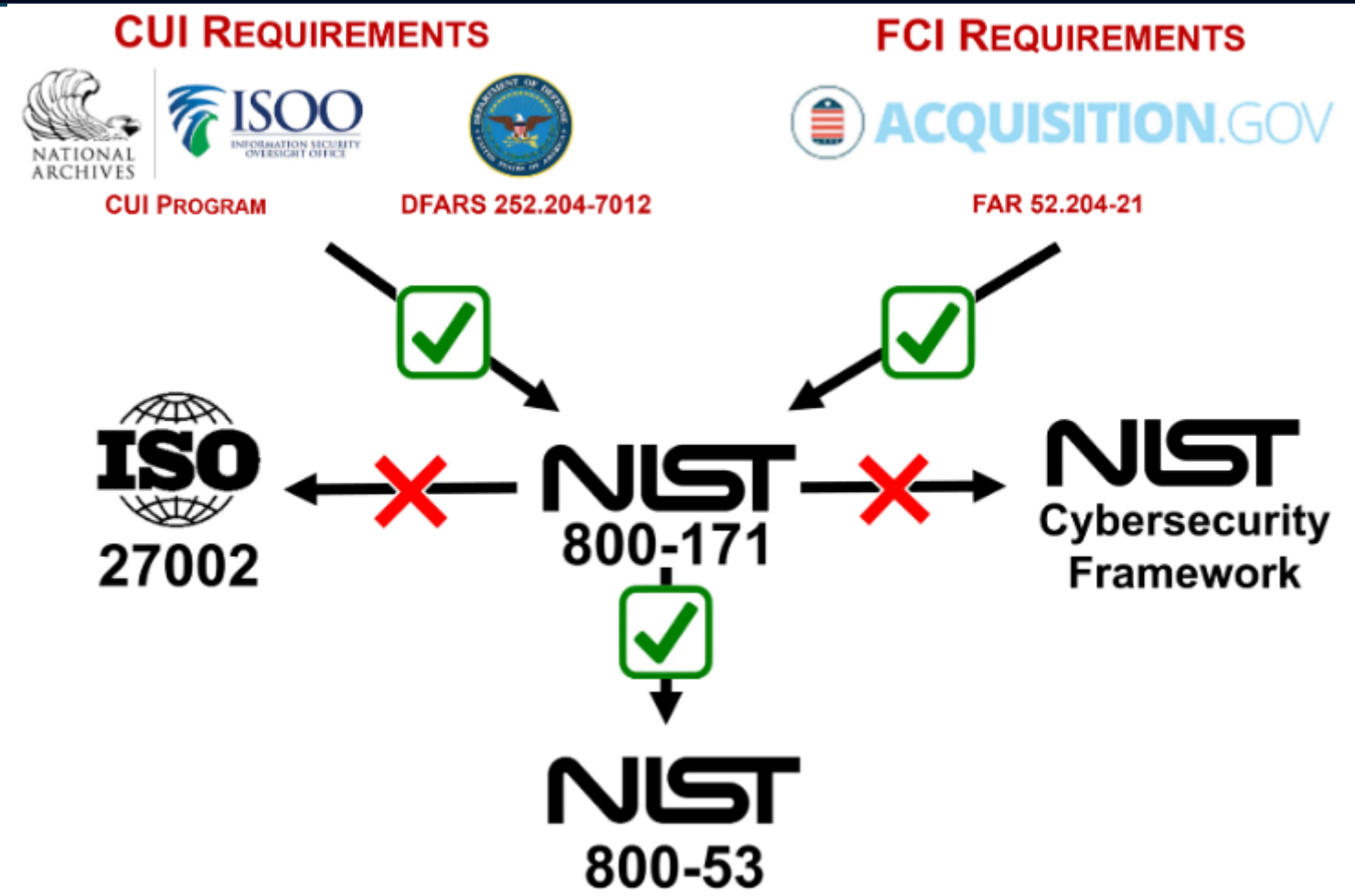
Breach involved a series of units, funded and operated by the PLA, identified as Advanced Persistent Threats (APT).

Targets were companies within Lockheed Martin's supply chain.

Data was primarily unclassified, but controlled, information.

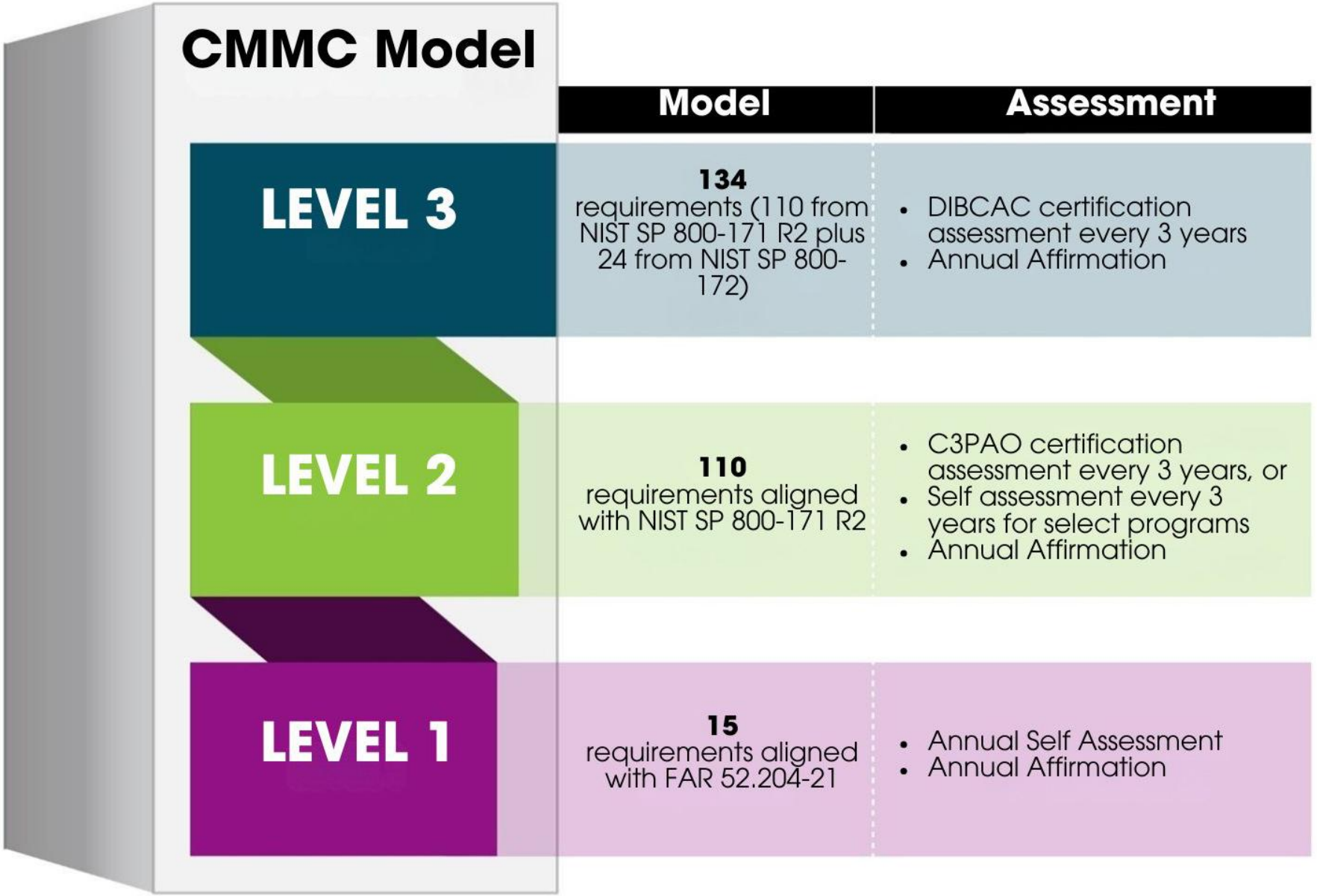

LOCKHEED MARTIN
3103

FAR 52.204-21, DFARS, NIST, and Beyond

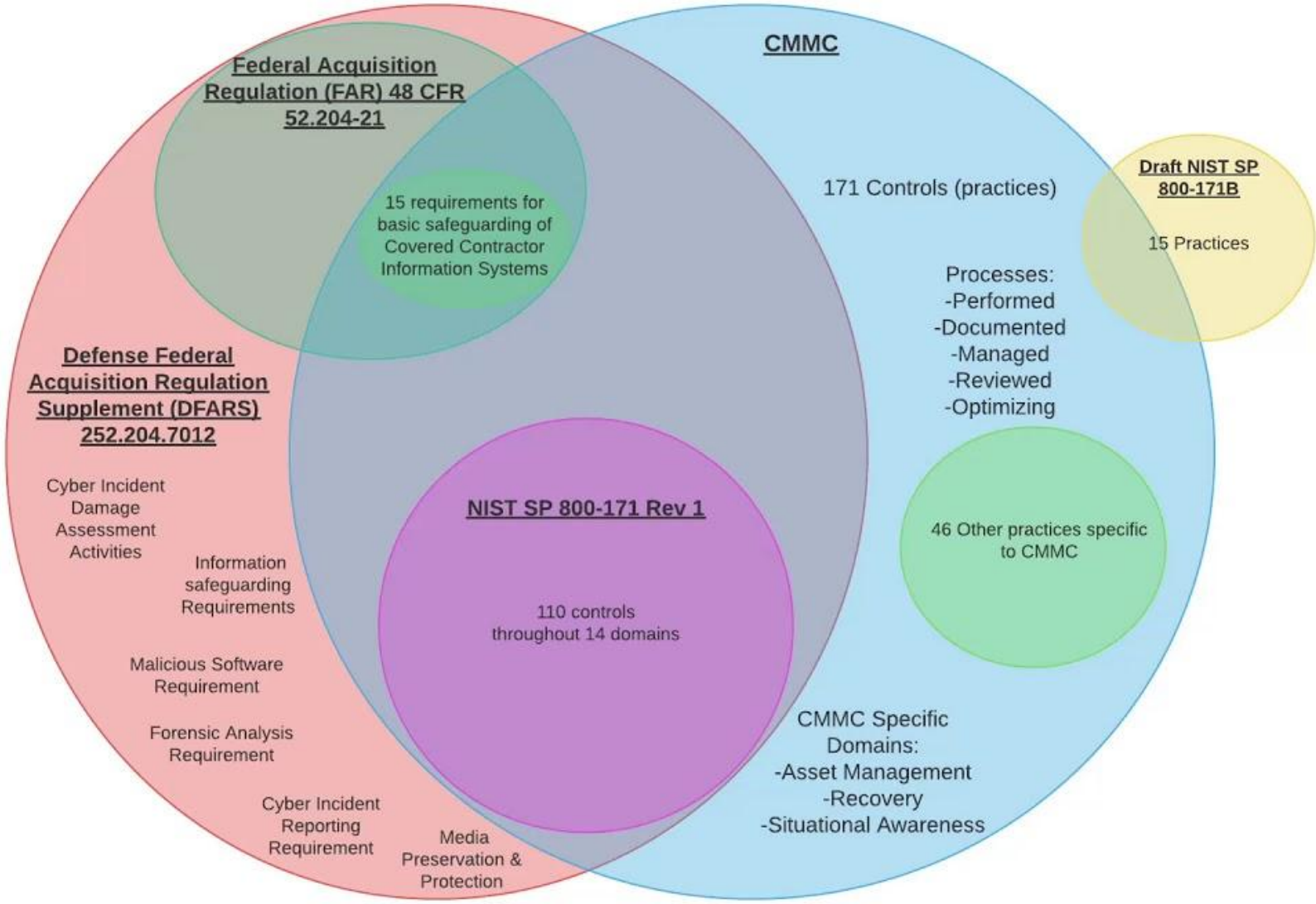


An Evolution – Not a Departure

CMMC 2.0


CMMC Model
Model
Assessment
LEVEL 3
134 requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)
DIBCAC certification assessment every 3 years
Annual Affirmation
LEVEL 2
110 requirements aligned with NIST SP 800-171 R2
C3PAO certification assessment every 3 years, or
Self assessment every 3 years for select programs
Annual Affirmation
LEVEL 1
15 requirements aligned with FAR 52.204-21
Annual Self Assessment
Annual Affirmation

FAR 52.204-21, DFARS, NIST, and Beyond



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.

1

CMMC Requirements By Level

2

NIST 800-171r2 Requirements

CMMC Levels

1

FOUNDATIONAL

An organization must demonstrate basic cyber hygiene practices, such as ensuring employees change passwords regularly to protect Federal Contract Information (FCI). FCI is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government."

2

ADVANCED

3

EXPERT

ACQUISITION.GOV

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

1 The FAR

https://www.acquisition.gov/far/52.204-21

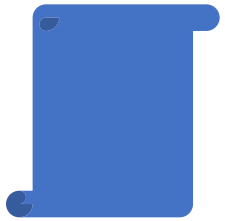
2 NIST SP 800-171A

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

3 DoD Memo

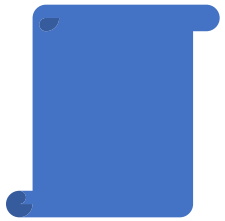
DoD Memo
DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements

Key Points



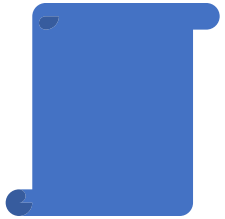
15 Controls

That cover “an inch deep but mile wide” through the information protection landscape.



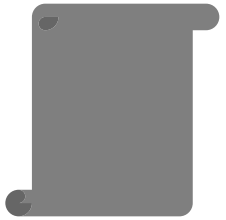
Are Echoed within NIST SP 800-171 Requirements

Complying with FAR 52.204-21 will always contribute to an attempt to comply with DFARS 252.204-7012



Considered Introductory

These controls represent minimal efforts, expense, and expertise to apply. “Common Sense” security.



They Are Maturing

CMMC Level 1 requirements will introduce a more formal approach to compliance with these controls.

The Controls

TABLE 1—CMMC LEVEL AND ASSESSMENT REQUIREMENTS

CMMC status	Source & number of security reqts.	Assessment reqts.	Plan of action & milestones (POA&M) reqts.	Affirmation reqts.
Level 1 (Self) ...	• 15 required by FAR clause 52.204–21.	• Conducted by Organization Seeking Assessment (OSA) annually. • Results entered into SPRS (or its successor capability).	• Not permitted	• After each assessment. • Entered into SPRS.

1. **Annual Self-Assessment**
2. **Results in SPRS**

The Controls

#	FAR 52.204-21 Cybersecurity Requirement	Control Type			Documentation Expectation		
		Technical	Administrative	Physical	Policies	Standards	Procedures
52.204-21(b)	Safeguarding requirements and procedures.	x	x	x	x	x	x
52.204-21(b)(1)	The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:		x		x	x	x
52.204-21(b)(1)(i)	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	x			x	x	x
52.204-21(b)(1)(ii)	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	x			x	x	x
52.204-21(b)(1)(iii)	Verify and control/limit connections to and use of external information systems.	x	x		x	x	x
52.204-21(b)(1)(iv)	Control information posted or processed on publicly accessible information systems.		x		x	x	x
52.204-21(b)(1)(v)	Identify information system users, processes acting on behalf of users, or devices.	x	x		x	x	x
52.204-21(b)(1)(vi)	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	x			x	x	x
52.204-21(b)(1)(vii)	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.		x	x	x	x	x
52.204-21(b)(1)(viii)	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.			x	x	x	x
52.204-21(b)(1)(ix)	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.		x	x	x	x	x
52.204-21(b)(1)(x)	Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	x	x		x	x	x
52.204-21(b)(1)(xi)	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	x			x	x	x
52.204-21(b)(1)(xii)	Identify, report, and correct information and information system flaws in a timely manner.	x	x		x	x	x
52.204-21(b)(1)(xiii)	Provide protection from malicious code at appropriate locations within organizational information systems.	x			x	x	x
52.204-21(b)(1)(xiv)	Update malicious code protection mechanisms when new releases are available.	x			x	x	x
52.204-21(b)(1)(xv)	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	x			x	x	x
52.204-21(b)(2)	Other requirements.This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.		x		x	x	x
52.204-21(c)	Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.		x		x	x	x

CMMC Levels

1

FOUNDATIONAL

2

ADVANCED

An organization must have an institutionalized management plan to implement good cyber hygiene practices to safeguard CUI, including all the NIST 800-171 r2 security requirements and processes.

3

EXPERT

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

DFARS 252.204-7012

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.

NATIONAL ARCHIVES

CONTROLLED UNCLASSIFIED INFORMATION

1

Definition

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls.

2

Categories

Archives.gov/cui/registry/category-list

3

Executive Agent

The National Archives and Records Administration.

CMMC Level 2

TABLE 1—CMMC LEVEL AND ASSESSMENT REQUIREMENTS

CMMC status	Source & number of security reqts.	Assessment reqts.	Plan of action & milestones (POA&M) reqts.	Affirmation reqts.
Level 2 (Self) ...	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by OSA every 3 years ..... • Results entered into SPRS (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).
Level 2 (C3PAO).	• 110 NIST SP 800–171 R2 required by DFARS clause 252.204–7012.	• Conducted by C3PAO every 3 years ..... • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) (or its successor capability). • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4.	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days. • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date.	• After each assessment and annually thereafter. • Assessment will lapse upon failure to annually affirm. • Entered into SPRS (or its successor capability).

Level 2 Self:

1. **Self-Assessment Every 3 Years**
2. **Results Entered into SPRS**
3. **POAM Not Permitted**
4. **Annual Affirmation**

Level 2 C3PAO:

1. **C3PAO Assessment Every 3 Years**
2. **Results Entered into SPRS**
3. **POAM Permitted (with limits)**
4. **Annual Affirmation**

Supplier Performance Risk System

- ❑ Level 1
- ❑ Level 2 (Self)
- ❑ Level 2 (C3PAO)
- ❑ Level 3

SPRS

SPRS stands for **Supplier Performance Risk System**, a DoD (Department of Defense) web-enabled application that provides performance information assessments for their acquisition community. It's the authorized source for retrieving supplier and product performance information, helping the DoD identify, assess, and monitor performance. SPRS supports DoD acquisition professionals in meeting regulatory and policy requirements by providing various risk assessments and data.

SPRS Instructions

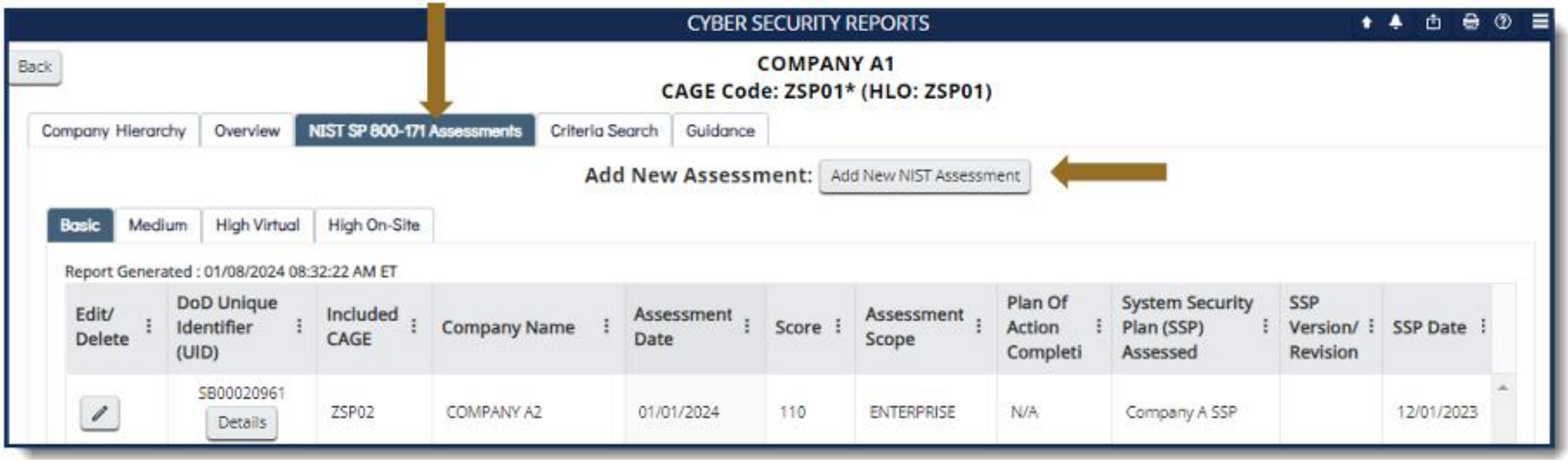
STEP 1

https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml

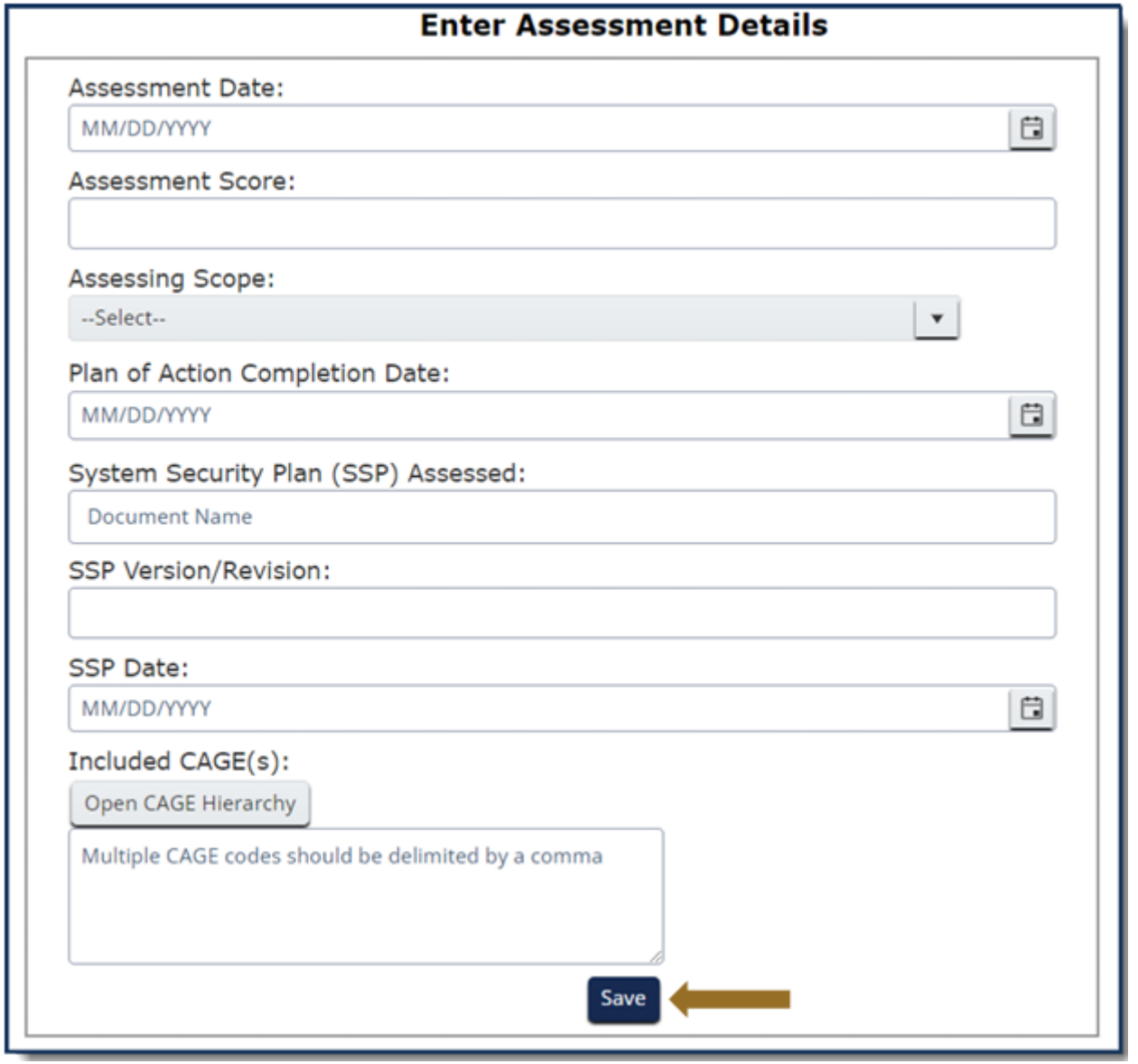
STEP 2

https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf

SPRS Instructions



SPRS Instructions



Supplier Performance Risk System

- ❑ Level 1
- ❑ **Level 2 (Self)**
- ❑ Level 2 (C3PAO)
- ❑ Level 3

Level 2 (Self)

Level 2 (Self) is a **self-assessment** to secure CUI processed, stored, or transmitted in the course of fulfilling the contract. The OSA must comply with the 110 Level 2 security requirements derived from **NIST SP 800-171 R2**.

NIST Handbook 162

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

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

DoD Memo

DoD Memo
DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements

Supplier Performance Risk System

- ❑ Level 1
- ❑ Level 2 (Self)
- ❑ **Level 2 (C3PAO)**
- ❑ Level 3

Level 2 (C3PAO)

Level 2 (C3PAO) differs from Level 2 (Self) in the method of verifying compliance. OSAs **must hire a C3PAO** to conduct an assessment of the OSA's compliance with the 110 security requirements of **NIST SP 800-171 R2**. OSAs can shop for C3PAOs on the CMMC Accreditation Body (AB) Marketplace.

NATIONAL ARCHIVES

FEDERAL REGISTER

The Daily Journal of the United States Government

DOCUMENT HEADINGS

Department of Defense
Office of the Secretary
32 CFR Part 170
[Docket ID: DoD-2023-OS-0063]
RIN 0790-AL49

1

CMMC Program

For verifying contractors have implemented security measures for FCI and CUI.

2

Tiered Implementation

Year 1: 135 Assessments
Year 2: 673 Assessments
Year 3: 2,252 Assessments
Year 4: 4,452 Assessments

3

Final Requirements

Level 1
Level 2 (Self)
Level 2 (C3PAO)
Level 3 (DIBCAC)

WPI Wisconsin Procurement Institute

APEX ACCELERATORS

CMMC Assessment

Pre-Assessment:

- Hire a C3PAO
- Provide SSP and Supporting Documentation
- Schedule Assessment

Assessment:

Interview

Examine

Test

Post Assessment:

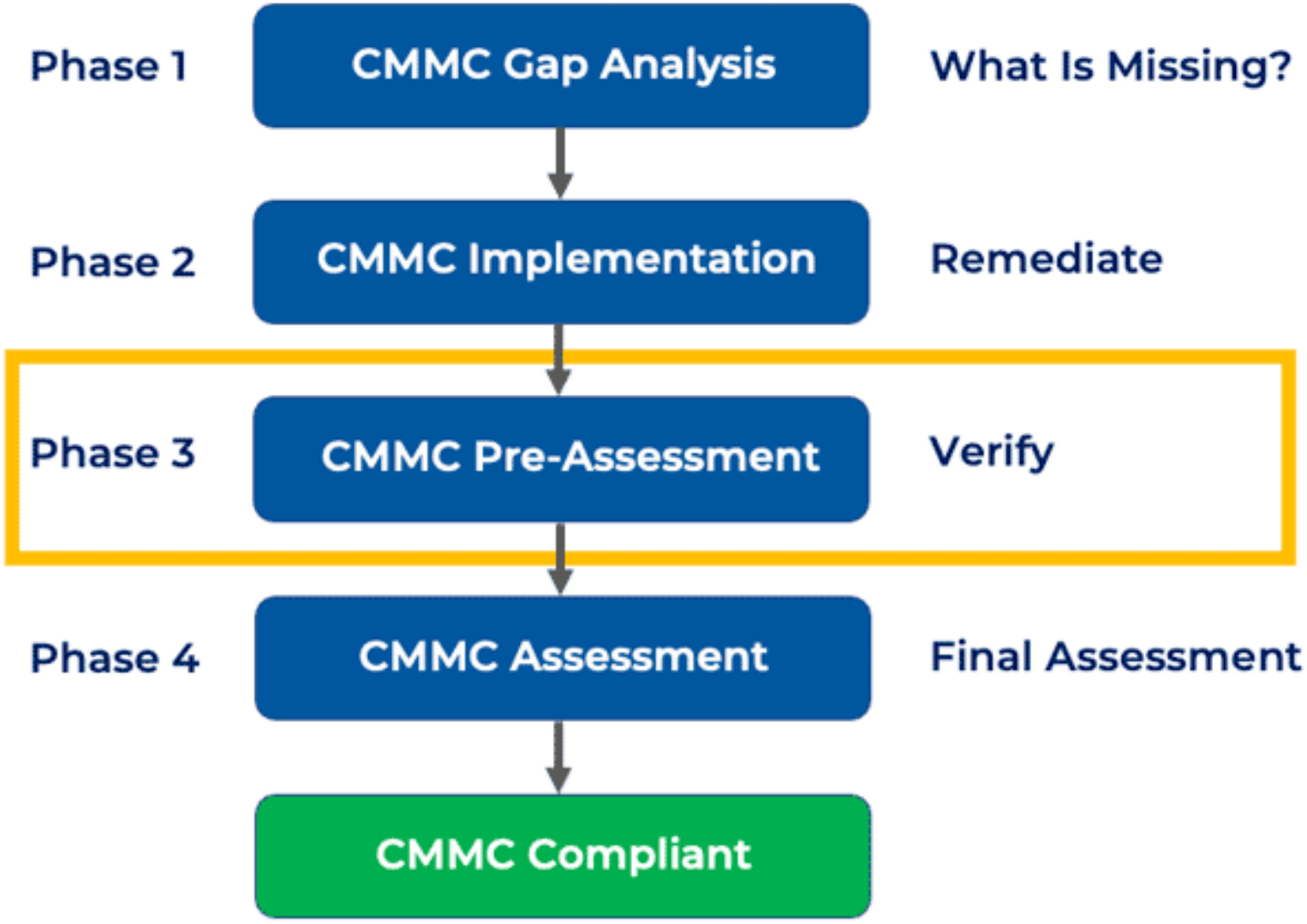
Submits report to Cyber-AB.

CMMC-AB performs quality check.

CMMC-AB issues report that confirms certification..

May allow limited use of POAM.

CMMC Assessment Timeline



CMMC L2 Assessment Phases

1. Plan and Prepare the Assessment
2. Conduct the Assessment
3. Report Assessment Results
4. Close-Out POA&Ms and Assessment

If the overall scoring of the Assessment after placing eligible items on the Limited Practice Deficiency Correction program results in **less than 80%** (88/110 practices “MET”), the OSC will receive a final finding of “Not Achieved” for CMMC Level 2 Certification. The OSC will be required to correct deficiencies and reapply for CMMC L2 Certification.

If the overall scoring of the Assessment after placing items on the Limited Practice Deficiency Correction program results in **greater than or equal to 80%** (88/110 practices “MET”), the OSC will be required to correct deficiencies.

Select C3PAO and Schedule

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

www.cyberab.org

1

CMMC Requirements By Level

2

NIST 800-171r2 Requirements

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**

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].

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].

3.11.1	**SECURITY REQUIREMENT** Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.1[a]	*the frequency to assess risk to organizational operations, organizational assets, and individuals is defined.*
	3.11.1[b]	*risk to organizational operations, organizational assets, and individuals resulting from the operation of an organizational system that processes, stores, or transmits CUI is assessed with the defined frequency.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; security planning policy and procedures; procedures addressing organizational risk assessments; system security plan; risk assessment; risk assessment results; risk assessment reviews; risk assessment updates; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Organizational processes for risk assessment; mechanisms supporting or for conducting, documenting, reviewing, disseminating, and updating the risk assessment].	

3.11.2	SECURITY REQUIREMENT Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.11.2[a]	*the frequency to scan for vulnerabilities in organizational systems and applications is defined.*
	3.11.2[b]	*vulnerability scans are performed on organizational systems with the defined frequency.*
	3.11.2[c]	*vulnerability scans are performed on applications with the defined frequency.*
	3.11.2[d]	*vulnerability scans are performed on organizational systems when new vulnerabilities are identified.*
	3.11.2[e]	*vulnerability scans are performed on applications when new vulnerabilities are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; system security plan; security assessment report; vulnerability scanning tools and associated configuration documentation; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with risk assessment, security assessment and vulnerability scanning responsibilities; personnel with vulnerability scan analysis and remediation responsibilities; personnel with information security responsibilities; system or network administrators].	

3.12.1	**SECURITY REQUIREMENT** Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.12.1[a] *the frequency of security control assessments is defined.*
	3.12.1[b] *security controls are assessed with the defined frequency to determine if the controls are effective in their application.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing security assessment planning; procedures addressing security assessments; security assessment plan; system security plan; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with security assessment responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Mechanisms supporting security assessment, security assessment plan development, and security assessment reporting].

3.12.2	**SECURITY REQUIREMENT** Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.12.2[a]	*deficiencies and vulnerabilities to be addressed by the plan of action are identified.*
	3.12.2[b]	*a plan of action is developed to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	3.12.2[c]	*the plan of action is implemented to correct identified deficiencies and reduce or eliminate identified vulnerabilities.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Security assessment and authorization policy; procedures addressing plan of action; system security plan; security assessment plan; security assessment report; security assessment evidence; plan of action; other relevant documents or records]. Interview: [*SELECT FROM:* Personnel with plan of action development and implementation responsibilities; personnel with information security responsibilities]. Test: [*SELECT FROM:* Mechanisms for developing, implementing, and maintaining plan of action].	

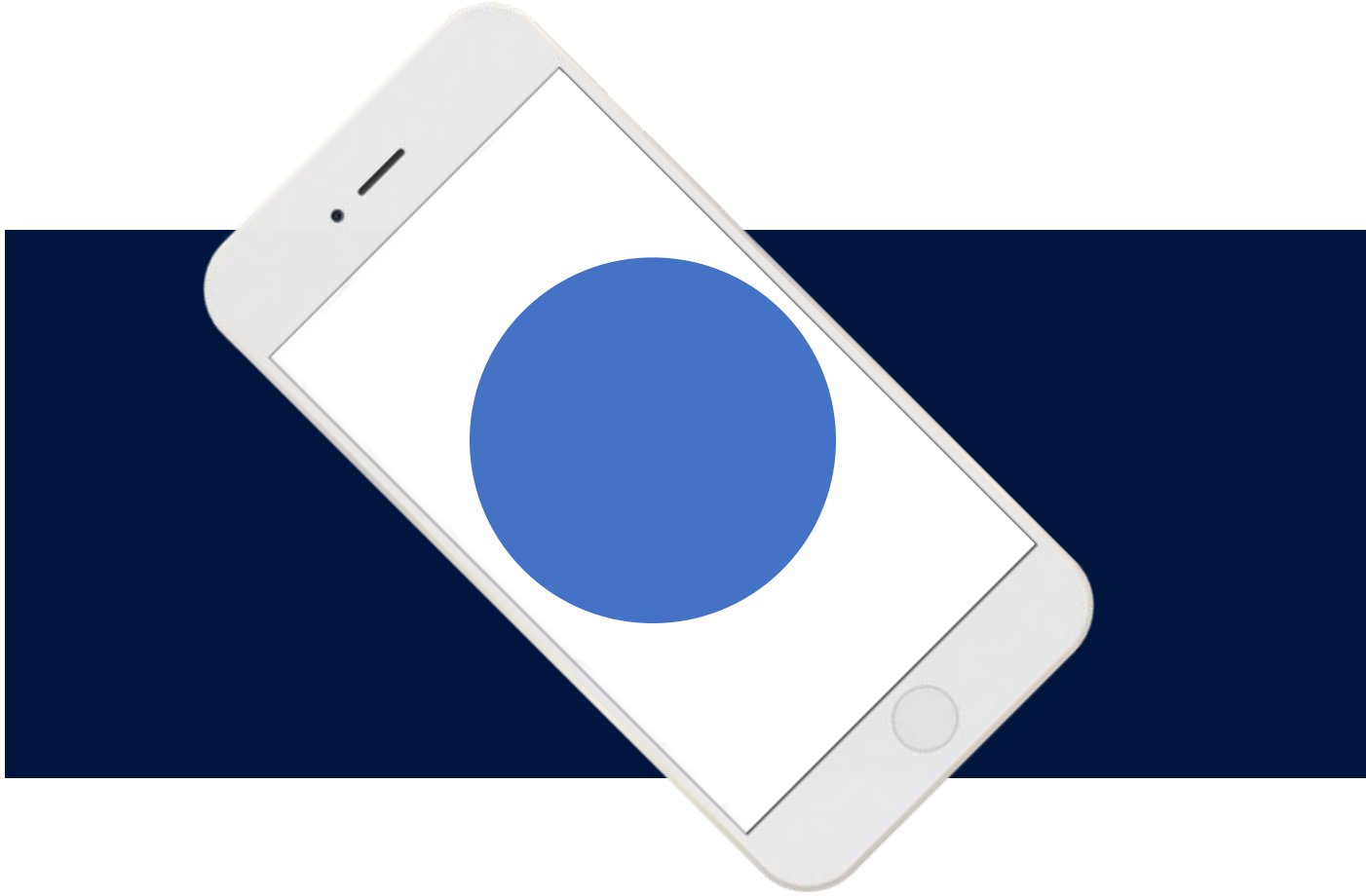
3.14.1	**SECURITY REQUIREMENT** Identify, report, and correct system flaws in a timely manner.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.1[a]	*the time within which to identify system flaws is specified.*
	3.14.1[b]	*system flaws are identified within the specified time frame.*
	3.14.1[c]	*the time within which to report system flaws is specified.*
	3.14.1[d]	*system flaws are reported within the specified time frame.*
	3.14.1[e]	*the time within which to correct system flaws is specified.*
	3.14.1[f]	*system flaws are corrected within the specified time frame.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* System and information integrity policy; procedures addressing flaw remediation; procedures addressing configuration management; system security plan; list of flaws and vulnerabilities potentially affecting the system; list of recent security flaw remediation actions performed on the system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct system flaws); test results from the installation of software and firmware updates to correct system flaws; installation/change control records for security-relevant software and firmware updates; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; personnel installing, configuring, and maintaining the system; personnel with responsibility for flaw remediation; personnel with configuration management responsibility]. Test: [*SELECT FROM:* Organizational processes for identifying, reporting, and correcting system flaws; organizational process for installing software and firmware updates; mechanisms supporting or implementing reporting, and correcting system flaws; mechanisms supporting or implementing testing software and firmware updates].	

Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

An APEX Accelerator



Upcoming Events

Cyber Friday

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.

- **April 25** – CMMC: Maintaining Your CMMC Certification
- **May 30** - Cybersecurity Rules You Need to Know to Work with the Federal Government / Department of Defense

…More information and registrations at wispro.org/events

Upcoming Events

May 14

Winning Government Business: Navigating Compliance Risks to Drive Strategic Advantage

Milwaukee, WI

May 15

11th Annual DOD Contract Management Update

Milwaukee, WI

…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

April 25 2025

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

mattf@wispro.org | 414-270-3600

10437 Innovation Drive Suite 320
Milwaukee WI 53226