Cyber Thursday

FAR 52.204-21: The Forgotten Baseline of Federal Cybersecurity

June 26 | 11:00 am – 12 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.

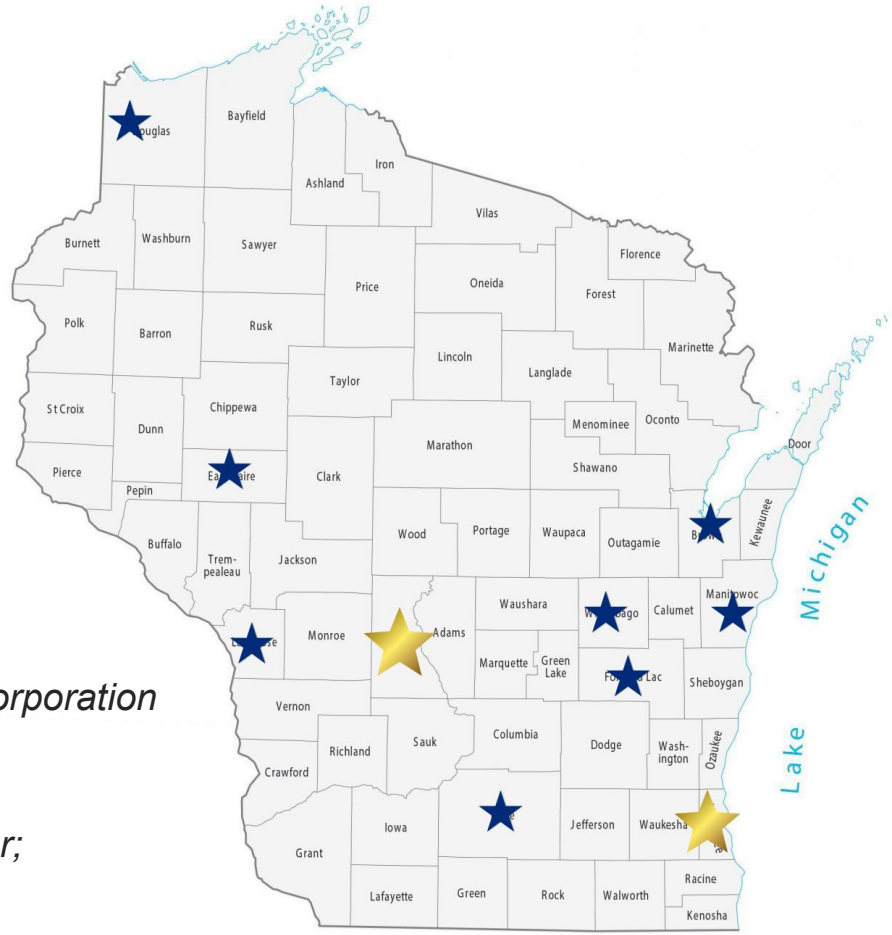
WPI provides services and training to all of Wisconsin's 72 counties

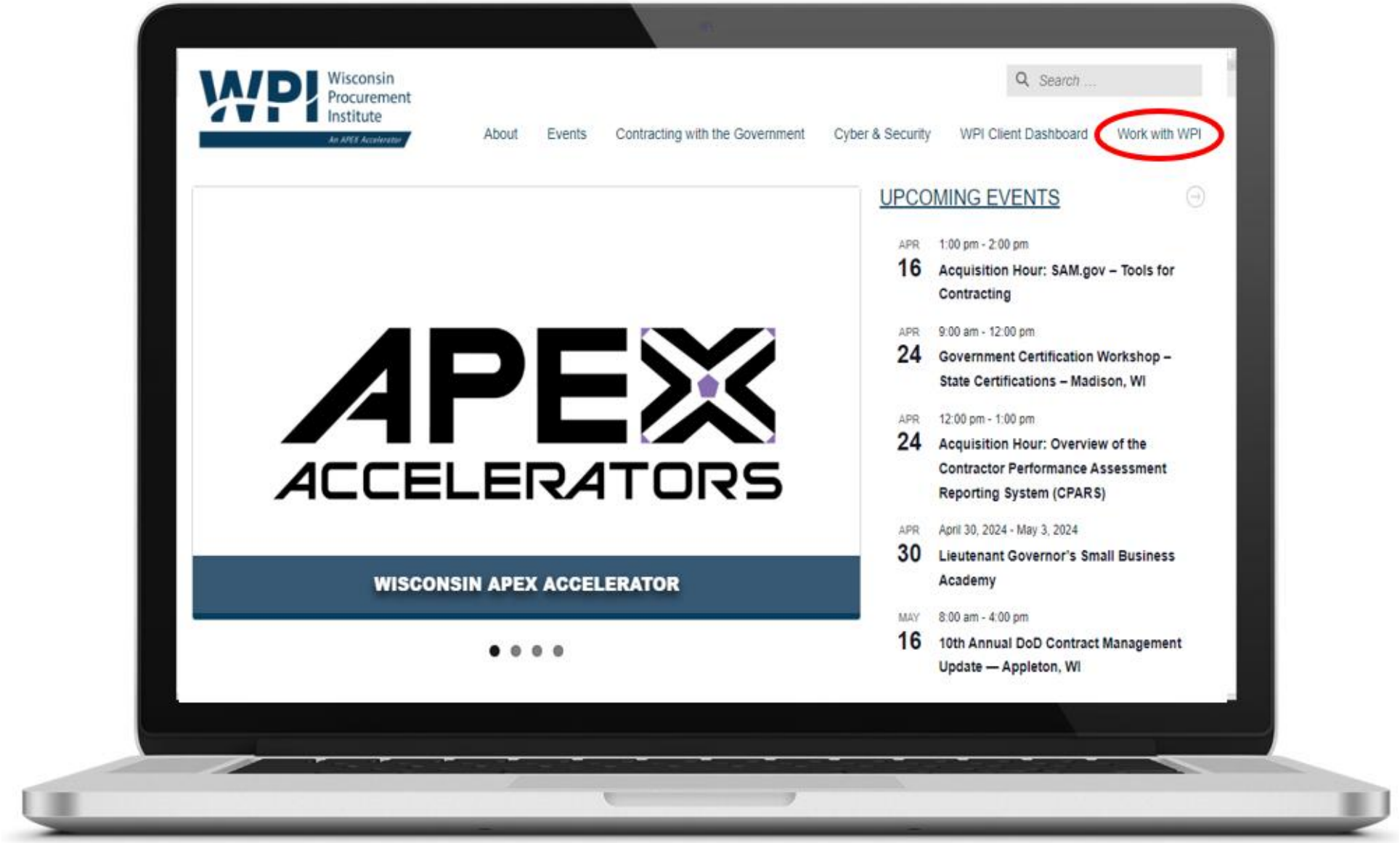
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting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

FAR 52.204-21 – The Forgotten Baseline

Wisconsin Procurement Institute

APEX ACCELERATORS

June 26th, 2025

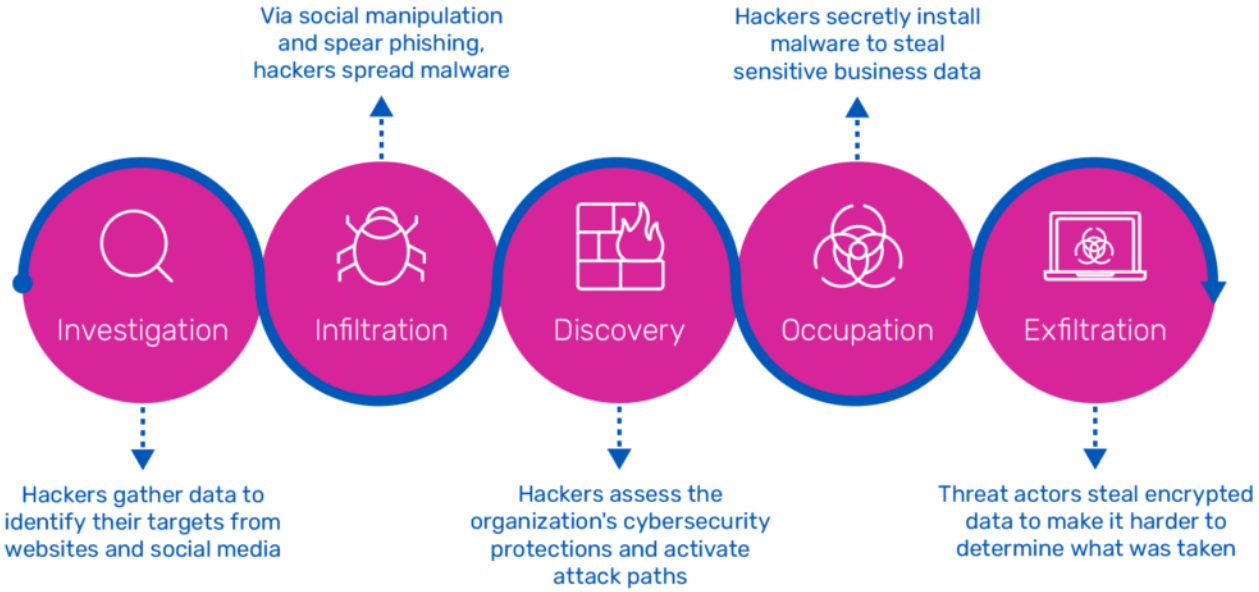
Confirmed in 2013, the theft of data from the F-35 Lightning II represented one of the largest data breaches in world history.

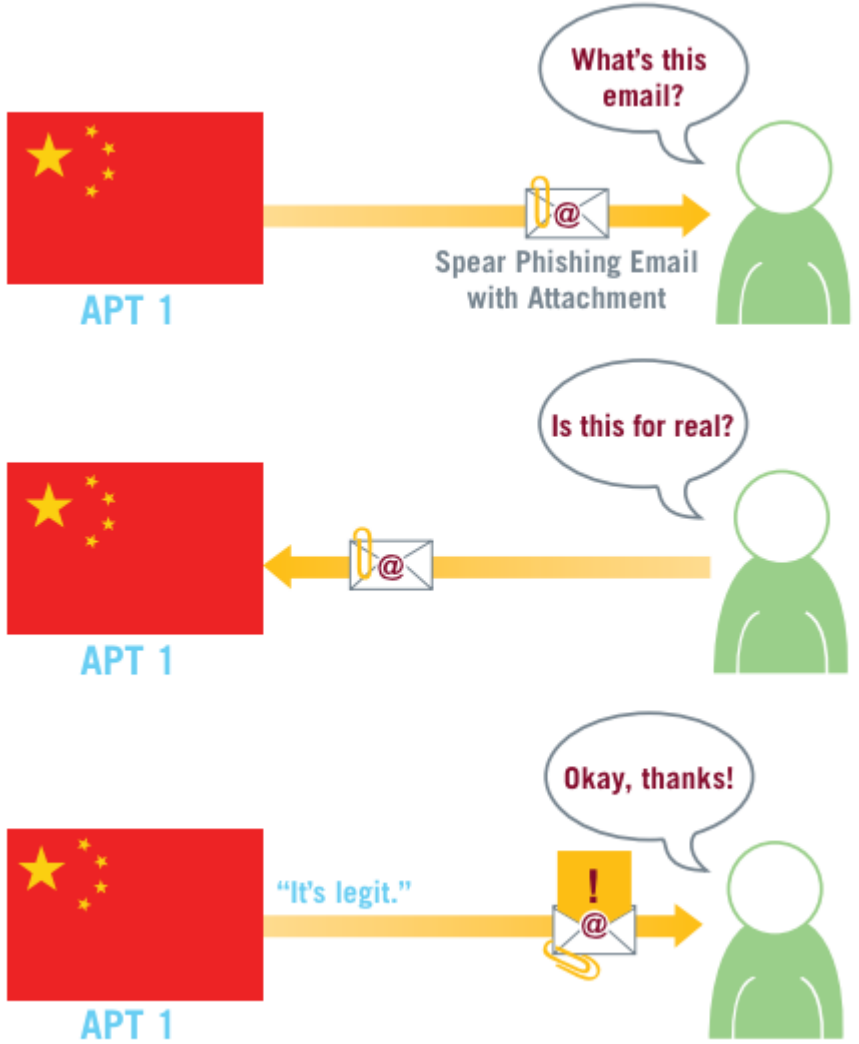
Breach involved a series of units, funded and operated by the PLA, identified as Advanced Persistent Threats (APT).

Targets were companies within Lockheed Martin's supply chain.

Data was primarily unclassified, but controlled, information.

What is an Advanced Persisent Threat?






LOCKHEED MARTIN
3103

1

FAR 52.204-21

2

What is FCI?

3

Requirements for Completion

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

FAR 52.204-21

The Contractor **shall** apply the following basic safeguarding requirements and procedures to protect covered contractor information systems.

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

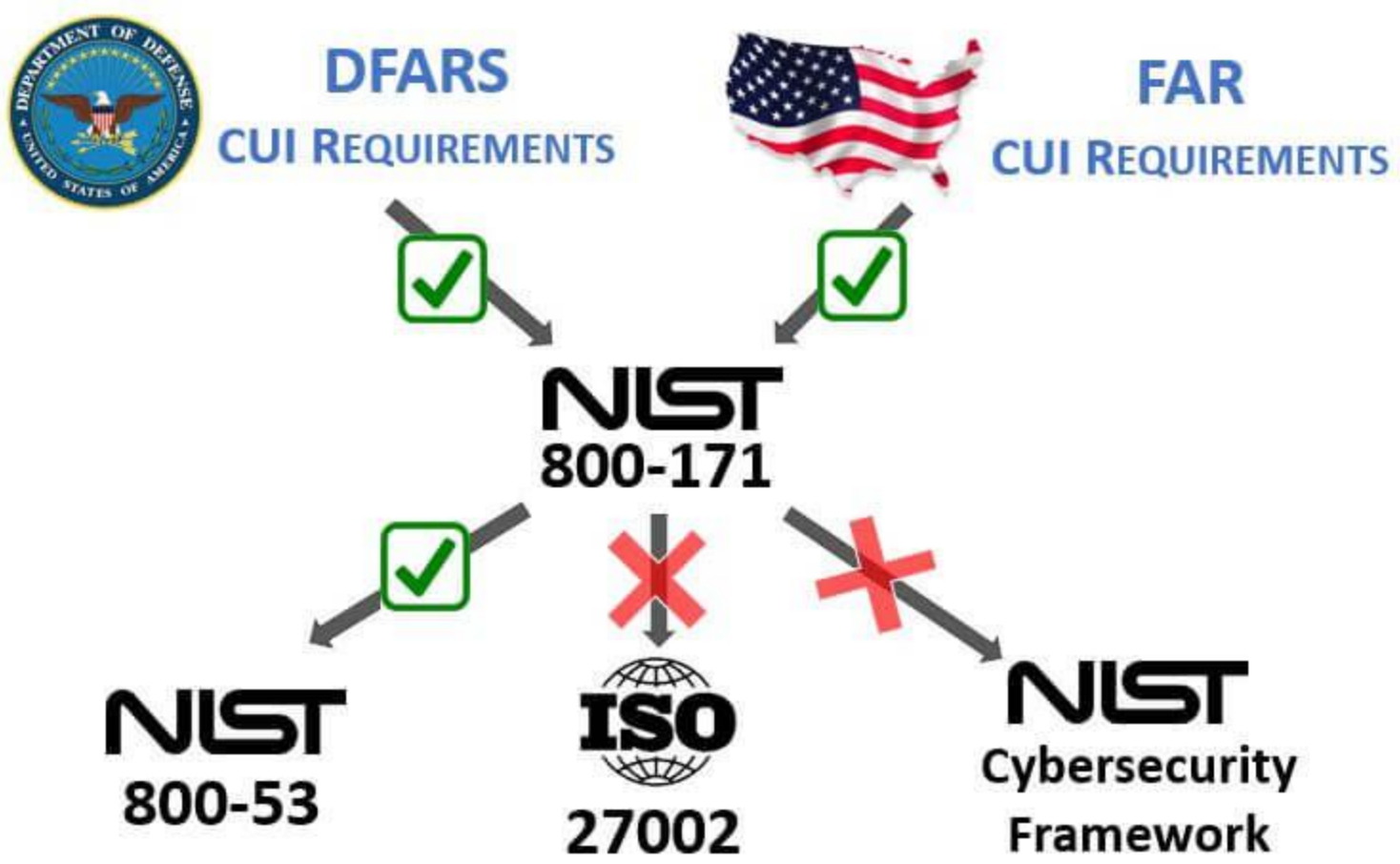
What is FCI?

Federal contract information (from 48 CFR 52.204-21) means 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**, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

15 Controls

- (i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- (ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- (iii) Verify and control/limit connections to and use of external information systems.
- (iv) Control information posted or processed on publicly accessible information systems.
- (v) Identify information system users, processes acting on behalf of users, or devices.
- (vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
- (vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
- (viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- (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.
- (xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
- (xii) Identify, report, and correct information and information system flaws in a timely manner.
- (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
- (xiv) Update malicious code protection mechanisms when new releases are available.
- (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

FAR 52.204-21, DFARS, NIST, and Beyond



An Evolution – Not a Departure

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.

1

FAR 52.204-21

2

What is FCI?

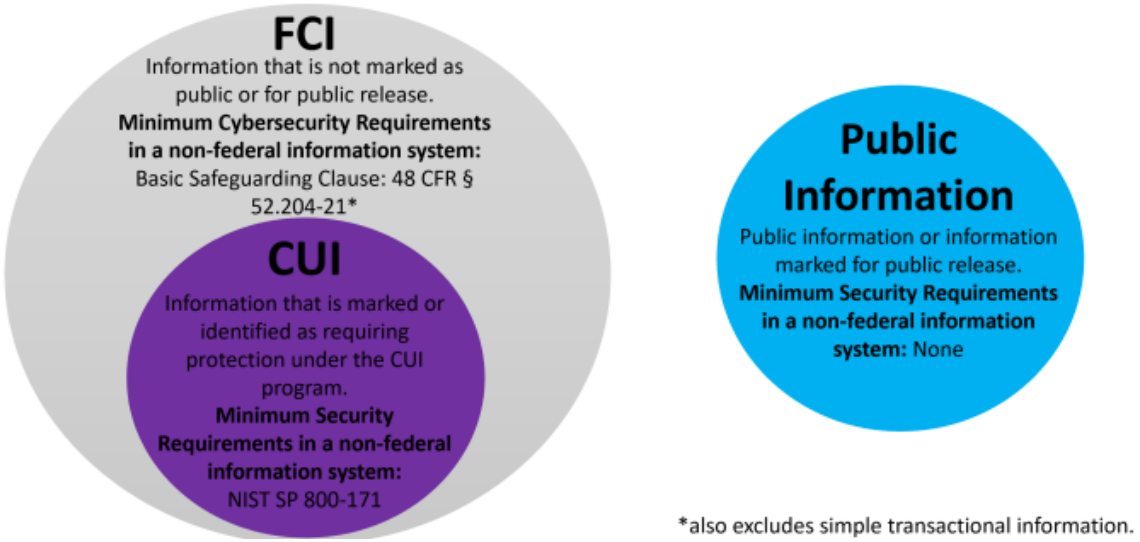
3

Requirements for Compliance

Paragraph C

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 products or commercial services**, 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.

Information that is collected, created, or received pursuant to a government contract



*also excludes simple transactional information.

1. Reports/Charts/Notes
2. Emails/Bills of Material
3. Contracts,
   Subcontracts,
   Purchase Orders

1

FAR 52.204-21

2

What is FCI?

3

Requirements for Compliance

Cybersecurity Timeline

START

2013

DFARS 252.204-7000 Rule goes into effect requiring the protection of sensitive data on non-federal systems.

JUN 2016

FAR 52.204-21 goes into effect.

DEC 2017

DFARS 252.204-7012 Rule goes into effected requiring all contract holders to self assess to meeting NIST SP 800-171.

OCT 2019

DoD announces the creation of the Cybersecurity Maturity Model Certification (CMMC) to transition from self-attestment to an outside certification of cyber hygeine.

NOV 2020

DFARS 2019-D041, intermin rule authorizing the inclusion of CMMC in procurement contracts.

Cybersecurity Timeline

DEC 8 2020

DOD and Cyber (Formerly CMMC)-AB release an updated timeline – stating the model has to be fully implemented by September 2021.

DEC 31 2020

General Services Administration acknowledges that while CMMC only applies currently to DOD contracts – ALL government contractors civilian or military should prepare to meet CMMC.

NOV 4 2021

DOD announces release of CMMC 2.0 – streamlining the additional requirements.

NOV 2023

CMMC Proposed Rule

Spring 2025!

Build a Program

#	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

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].

3.1.2	**SECURITY REQUIREMENT** Limit system access to the types of transactions and functions that authorized users are permitted to execute.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.2[a]	*the types of transactions and functions that authorized users are permitted to execute are defined.*
	3.1.2[b]	*system access is limited to the defined types of transactions and functions for authorized users.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing access enforcement; system security plan; system design documentation; list of approved authorizations including remote access authorizations; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with access enforcement responsibilities; system or network administrators; personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Mechanisms implementing access control policy].	

3.1.20	**SECURITY REQUIREMENT** Verify and control/limit connections to and use of external systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.1.20[a] *connections to external systems are identified.*
	3.1.20[b] *the use of external systems is identified.*
	3.1.20[c] *connections to external systems are verified.*
	3.1.20[d] *the use of external systems is verified.*
	3.1.20[e] *connections to external systems are controlled/limited.*
	3.1.20[f] *the use of external systems is controlled/limited.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the use of external systems; terms and conditions for external systems; system security plan; list of applications accessible from external systems; system configuration settings and associated documentation; system connection or processing agreements; account management documents; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for defining terms and conditions for use of external systems to access organizational systems; system or network administrators; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing terms and conditions on use of external systems].

3.1.22	**SECURITY REQUIREMENT** Control CUI posted or processed on publicly accessible systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.22[a]	*individuals authorized to post or process information on publicly accessible systems are identified.*
	3.1.22[b]	*procedures to ensure CUI is not posted or processed on publicly accessible systems are identified.*
	3.1.22[c]	*a review process is in place prior to posting of any content to publicly accessible systems.*
	3.1.22[d]	*content on publicly accessible systems is reviewed to ensure that it does not include CUI.*
	3.1.22[e]	*mechanisms are in place to remove and address improper posting of CUI.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Access control policy; procedures addressing publicly accessible content; system security plan; list of users authorized to post publicly accessible content on organizational systems; training materials and/or records; records of publicly accessible information reviews; records of response to nonpublic information on public websites; system audit logs and records; security awareness training records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with responsibilities for managing publicly accessible information posted on organizational systems; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing management of publicly accessible content].	

3.5.1	**SECURITY REQUIREMENT** Identify system users, processes acting on behalf of users, and devices.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.5.1[a] *system users are identified.*
	3.5.1[b] *processes acting on behalf of users are identified.*
	3.5.1[c] *devices accessing the system are identified.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; system security plan, system design documentation; system configuration settings and associated documentation; system audit logs and records; list of system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with system operations responsibilities; personnel with information security responsibilities; system or network administrators; personnel with account management responsibilities; system developers]. **Test**: [*SELECT FROM:* Organizational processes for uniquely identifying and authenticating users; mechanisms supporting or implementing identification and authentication capability].

3.5.2	**SECURITY REQUIREMENT** Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.5.2[a] *the identity of each user is authenticated or verified as a prerequisite to system access.*
	3.5.2[b] *the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access.*
	3.5.2[c] *the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Identification and authentication policy; system security plan; procedures addressing authenticator management; procedures addressing user identification and authentication; system design documentation; list of system authenticator types; system configuration settings and associated documentation; change control records associated with managing system authenticators; system audit logs and records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with authenticator management responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Mechanisms supporting or implementing authenticator management capability].

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.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System media protection policy; procedures addressing media sanitization and disposal; applicable standards and policies addressing media sanitization; system security plan; media sanitization records; system audit logs and records; system design documentation; system configuration settings and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with media sanitization responsibilities; personnel with information security responsibilities; system or network administrators]. **Test**: [*SELECT FROM:* Organizational processes for media sanitization; mechanisms supporting or implementing media sanitization].

3.10.1	**SECURITY REQUIREMENT** Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.1[a] *authorized individuals allowed physical access are identified.*
	3.10.1[b] *physical access to organizational systems is limited to authorized individuals.*
	3.10.1[c] *physical access to equipment is limited to authorized individuals.*
	3.10.1[d] *physical access to operating environments is limited to authorized individuals.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access authorizations; system security plan; authorized personnel access list; authorization credentials; physical access list reviews; physical access termination records and associated documentation; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with physical access authorization responsibilities; personnel with physical access to system facility; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for physical access authorizations; mechanisms supporting or implementing physical access authorizations].

3.10.3	**SECURITY REQUIREMENT** Escort visitors and monitor visitor activity.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.3[a] *visitors are escorted.*
	3.10.3[b] *visitor activity is monitored.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with physical access control responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

3.10.4	**SECURITY REQUIREMENT** Maintain audit logs of physical access.
	ASSESSMENT OBJECTIVE *Determine if audit logs of physical access are maintained.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with physical access control responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

3.10.5	**SECURITY REQUIREMENT** Control and manage physical access devices.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.10.5[a] *physical access devices are identified.*
	3.10.5[b] *physical access devices are controlled.*
	3.10.5[c] *physical access devices are managed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* Physical and environmental protection policy; procedures addressing physical access control; system security plan; physical access control logs or records; inventory records of physical access control devices; system entry and exit points; records of key and lock combination changes; storage locations for physical access control devices; physical access control devices; list of security safeguards controlling access to designated publicly accessible areas within facility; other relevant documents or records]. **Interview**: [*SELECT FROM:* Personnel with physical access control responsibilities; personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for physical access control; mechanisms supporting or implementing physical access control; physical access control devices].

3.13.1	**SECURITY REQUIREMENT** Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.
	ASSESSMENT OBJECTIVE *Determine if:*

3.13.1[a]	*the external system boundary is defined.*
3.13.1[b]	*key internal system boundaries are defined.*
3.13.1[c]	*communications are monitored at the external system boundary.*
3.13.1[d]	*communications are monitored at key internal boundaries.*
3.13.1[e]	*communications are controlled at the external system boundary.*
3.13.1[f]	*communications are controlled at key internal boundaries.*
3.13.1[g]	*communications are protected at the external system boundary.*
3.13.1[h]	*communications are protected at key internal boundaries.*

POTENTIAL ASSESSMENT METHODS AND OBJECTS

Examine: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; enterprise security architecture documentation; system audit logs and records; system configuration settings and associated documentation; other relevant documents or records].

Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developer; personnel with boundary protection responsibilities].

Test: [*SELECT FROM:* Mechanisms implementing boundary protection capability].

3.13.5	**SECURITY REQUIREMENT** Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.13.5[a] *publicly accessible system components are identified.*
	3.13.5[b] *subnetworks for publicly accessible system components are physically or logically separated from internal networks.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and communications protection policy; procedures addressing boundary protection; system security plan; list of key internal boundaries of the system; system design documentation; boundary protection hardware and software; system configuration settings and associated documentation; enterprise security architecture 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; personnel with boundary protection responsibilities]. **Test**: [*SELECT FROM:* Mechanisms implementing boundary protection capability].

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].

3.14.2	**SECURITY REQUIREMENT** Provide protection from malicious code at designated locations within organizational systems.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.14.2[a]	*designated locations for malicious code protection are identified.*
	3.14.2[b]	*protection from malicious code at designated locations is provided.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; records of malicious code protection updates; malicious code protection mechanisms; system security plan; system configuration settings and associated documentation; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; scan results from malicious code protection mechanisms; system design documentation; system audit logs and records; other relevant documents or records].	

3.14.4	**SECURITY REQUIREMENT** Update malicious code protection mechanisms when new releases are available.
	ASSESSMENT OBJECTIVE *Determine if malicious code protection mechanisms are updated when new releases are available.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; 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 malicious code protection; personnel with configuration management responsibility].

3.14.5	**SECURITY REQUIREMENT** Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
	ASSESSMENT OBJECTIVE *Determine if:*
	3.14.5[a] *the frequency for malicious code scans is defined.*
	3.14.5[b] *malicious code scans are performed with the defined frequency.*
	3.14.5[c] *real-time malicious code scans of files from external sources as files are downloaded, opened, or executed are performed.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS **Examine**: [*SELECT FROM:* System and information integrity policy; configuration management policy and procedures; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; system security plan; system design documentation; system configuration settings and associated documentation; scan results from malicious code protection mechanisms; record of actions initiated by malicious code protection mechanisms in response to malicious code detection; system audit logs and records; 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 malicious code protection; personnel with configuration management responsibility]. **Test**: [*SELECT FROM:* Organizational processes for employing, updating, and configuring malicious code protection mechanisms; organizational process for addressing false positives and resulting potential impact; mechanisms supporting or implementing malicious code protection mechanisms (including updates and configurations); mechanisms supporting or implementing malicious code scanning and subsequent actions].

DFARS 252.204-7021

Cybersecurity Maturity Model Certification Requirements

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

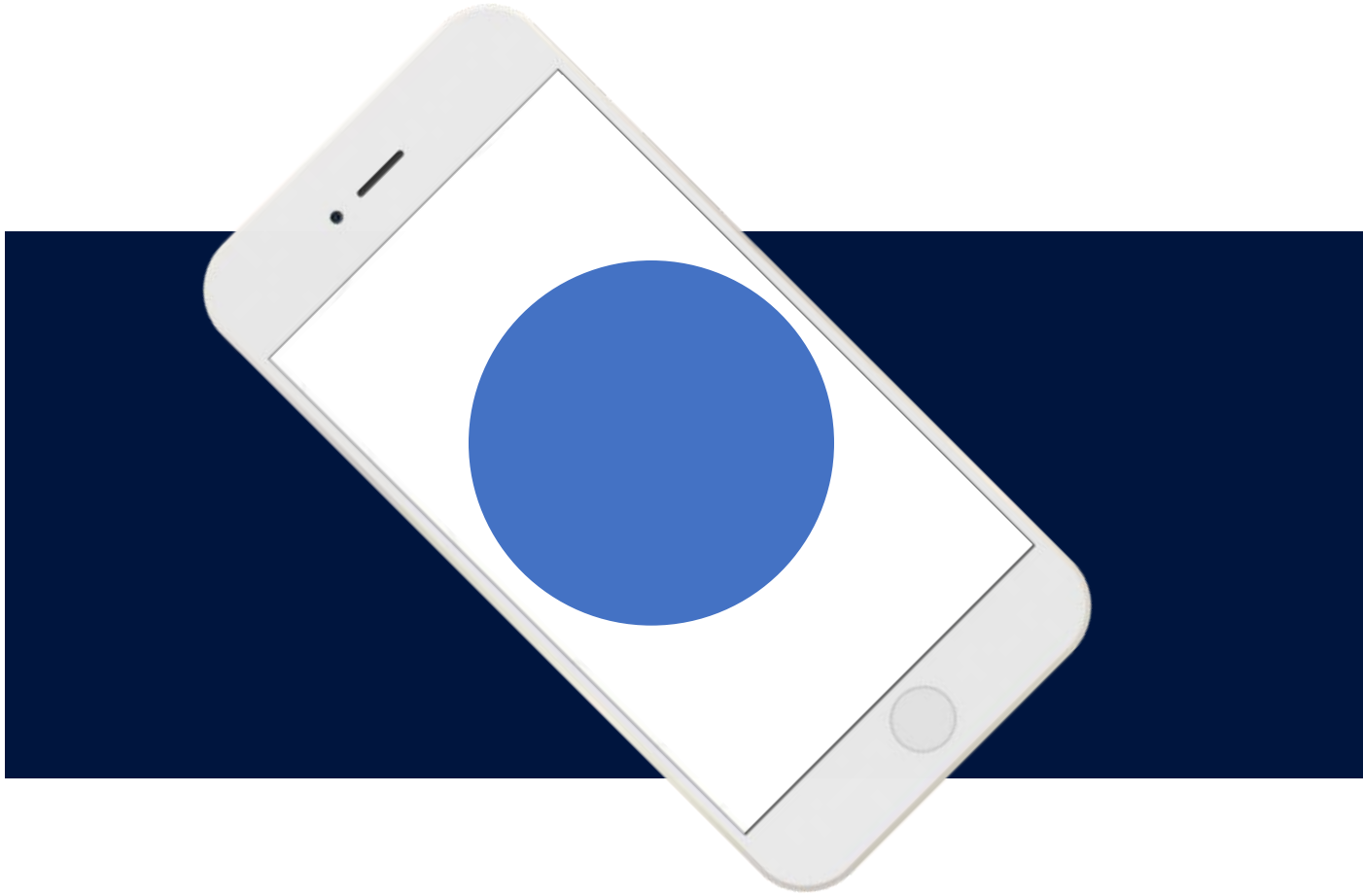
An organization must have an institutionalized management plan to implement good cyber hygiene practices to safeguard CUI, including all the NIST 800-171 r2 security requirements and processes.

3 EXPERT

An organization must have standardized and optimized processes in place and additional enhanced practices that detect and respond to changing tactics, techniques and procedures (TTPs) of advanced persistent threats (APTs). An APT is as an adversary that possesses sophisticated levels of cyber expertise and significant resources to conduct attacks from multiple vectors. Capabilities include having resources to monitor, scan, and process data forensics..

WPI Wisconsin Procurement Institute

APEX ACCELERATORS



APEX ACCELERATORS

Upcoming Events

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.

- **June 25** – How to Analyze Federal Solicitation
- **July 9** – Writing a Winning Government Proposal
- **July 23** – Federal Invoicing: PIEE / Wide Area Workflow
- **August 6** – Writing an Effective Capabilities Statement
- **August 20** – End of the Federal Fiscal Year Spending: Are You Ready?

…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.

- **June 26** – FAR 52.204-21: The Forgotten Baseline of Federal Cybersecurity
- **July 31** – CMMC 2.0: What Contractors Must Know in 2025
- **August 28** – The Federal Cybersecurity Horizon: Zero Trust, FedRAMP, & Supply Chain Risk

…More information and registrations at wispro.org/events

19th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In Partnership with Wisconsin's Military Installations

July 9
Truax Field

July 30
Fort McCoy

GOBC will provide you the opportunity to gain insights into:

- ***COFFEE with the COMMANDER***
- Current operations and priorities at Wisconsin's Federal and State government agencies and military facilities
- Connecting with agency and installation leadership, operational staff and buyers
- Locating and bidding on current and future procurement opportunities
- Resources available to assist your business in winning government prime and subcontracts

…More information and registrations at wispro.org/events

…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

June 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