

Cyber Thursday:

Cybersecurity Requirements for Non-Department of War Contractors and Suppliers

July 9 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute





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 Thursdays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more.....

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**

- *Technology Innovation Center*

- **MADISON**

- *FEED Kitchens*
- *Dane County Latino Chamber of Commerce*
- *Madison Area Technical College (MATC)*

- **CAMP DOUGLAS**

- *Juneau County Economic Development Corporation (JCEDC)*

- **EAU CLAIRE**

- *Western Dairyland*

- **FOND DU LAC**

- *Envision Greater Fond du Lac*

- **GREEN BAY**

- *NWTC Startup Hub*

- **LACROSSE**

- *La Crosse Public Library*

- **MANITOWOC**

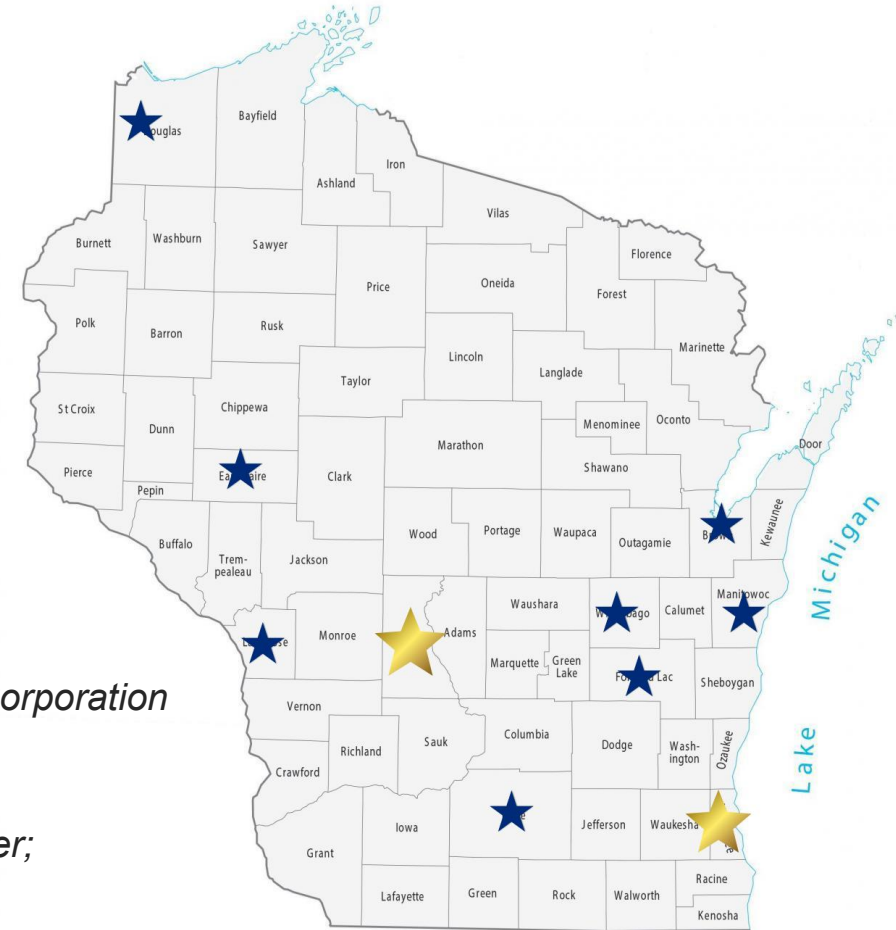
- *Progress Lakeshore*

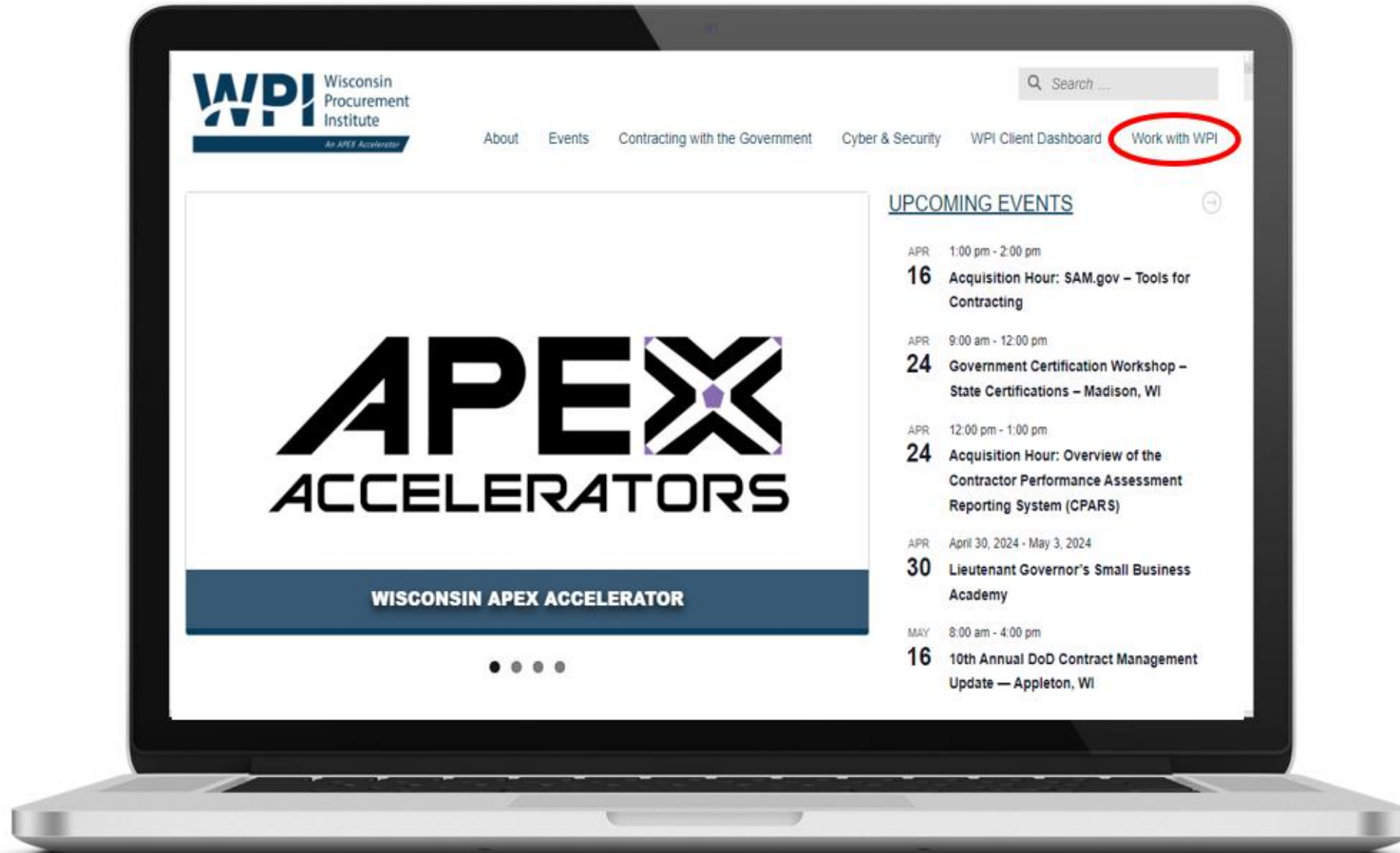
- **OSHKOSH**

- *Greater Oshkosh
Economic Development Corporation*

- **SUPERIOR**

- *Small Business Dev Center;
UW Superior*

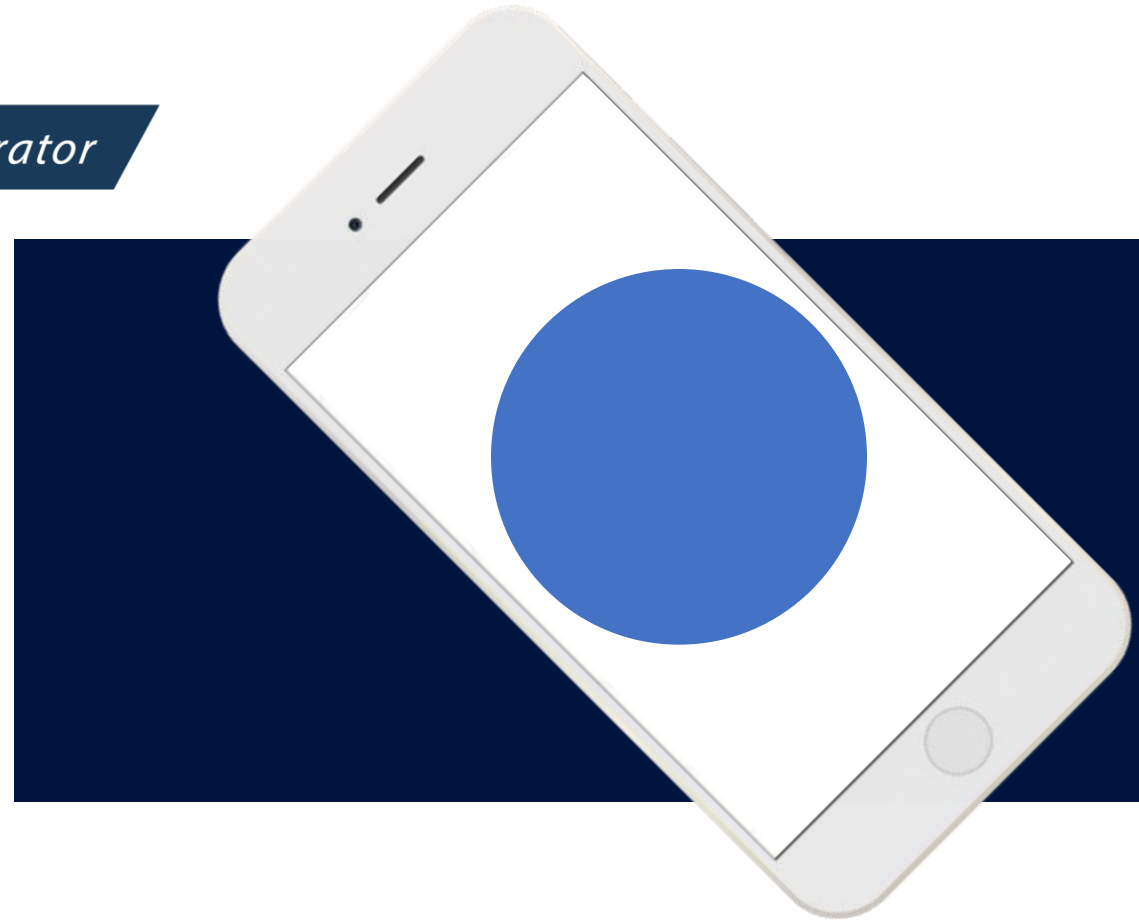






An APEX Accelerator

Requirements for Non-DOW Contractors and Suppliers



Cyber Thursday – July 9th, 2026

Why This Session Matters Right Now

2026

Cybersecurity Requirements are being highlighted across the Federal landscape.

GSA released a new CMMC-like framework in January; the FAR CUI rule was significantly revised in June.

THREE THINGS THAT CHANGED IN THE LAST 12 MONTHS

GSA introduced a CMMC-like framework for civilian contractors — January 2026

Requires NIST SP 800-171 Rev 3, third-party assessment, and one-hour incident reporting. No transition period. Applies at contracting officer discretion in new solicitations.

The FAR CUI rule was significantly revised — June 2026

Now sits in new FAR Part 40, uses new clauses 52.240-6 and 52.240-7 and Standard Form XXX, requires NIST 800-171 Rev 3, and 72-hour incident reporting. Final rule expected by end of 2026 with no phase-in.

Sector rules and state laws continue to expand

FTC Safeguards Rule reach keeps growing; state breach notification laws add teeth every year; cyber insurance carriers require the same controls contracts do.

What We'll Cover

1

The Landscape

Why non-DoW cybersecurity requirements changed dramatically in 2025-2026

2

The Foundation

FCI, CUI, and FAR 52.204-21 — the requirements that already apply to every federal contractor

3

GSA's New CUI Framework

The January 2026 procedural guide — NIST 800-171 Rev 3, showstoppers, one-hour reporting

4

The FAR CUI Rule

The June 2026 revised proposed rule — new FAR Part 40, SF XXX, and clauses 52.240-6 and 52.240-7

5

Other Requirements That May Apply

Sector rules, state laws, cybersecurity insurance

6

Decision Framework

How to figure out what actually applies to your business

7

Getting Ready

Practical starting points and where to get help

SECTION 1 • THE LANDSCAPE

Why Non-DoW Contractors Should Care Now

The world where civilian-agency cybersecurity was optional is ending.



The Old World vs. The New World

The Old World (through ~2024)

DoD only: Detailed cybersecurity requirements applied mainly to defense contractors — DFARS 252.204-7012, NIST 800-171, CMMC

Civilian minimum: Non-defense contractors met FAR 52.204-21 — 15 basic safeguarding requirements; enforcement was largely self-attestation

Agency patchwork: Civilian agencies added ad-hoc cybersecurity clauses to individual contracts; no consistent framework

Enforcement: Rare — mostly triggered by breaches, whistleblower actions, or False Claims Act cases

The New World (2025–2026 forward)

GSA framework: New CMMC-like process for GSA contractors handling CUI — third-party assessment, Rev 3 controls, one-hour reporting

FAR CUI rule: Coming government-wide — will apply to all federal contracts involving CUI, defense or civilian

Standardization: New Standard Form XXX identifies CUI in every solicitation; consistent clauses replace the ad-hoc patchwork

Enforcement: False Claims Act cyber-fraud initiative growing; DOJ recovered \$52M in FY25 alone from cybersecurity settlements

Three Shifts Reshaping the Non-DoW Landscape

THE BIG IDEA

The last 18 months delivered more federal cybersecurity change for civilian contractors than the previous decade combined. These three trends explain most of what's coming.

1

SHIFT 1

Civilian Catches Up

GSA's January 2026 procedural guide put civilian contractors on a NIST 800-171 Rev 3 baseline with mandatory third-party assessment — the first major framework to do so. Other agencies are expected to follow.

2

SHIFT 2

Standardization Coming

The revised FAR CUI rule (June 2026) creates one uniform mechanism — Standard Form XXX plus FAR clauses 52.240-6 and 52.240-7 — for every federal contract involving CUI, replacing agency-by-agency patchwork.

3

SHIFT 3

The Stakes Are Rising

Cybersecurity is no longer a check-the-box item. False Claims Act settlements, contract-level enforcement, and insurance market pressure are turning cyber posture into an existential business issue.

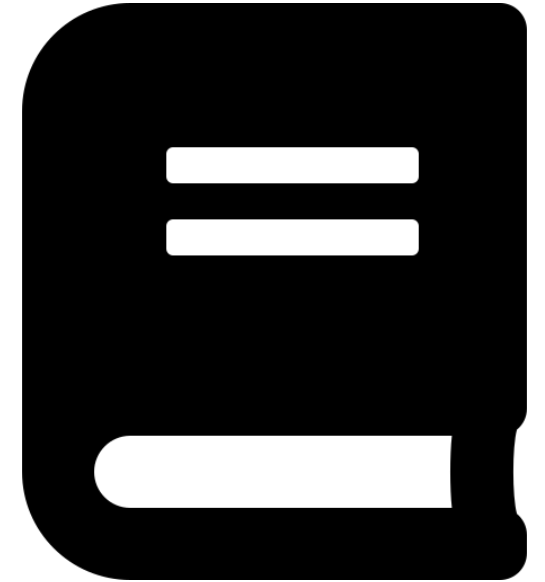
BOTTOM LINE

If your business touches federal contracts, **even indirectly as a subcontractor**, the requirements you'll face in 2027 look very different from the ones you faced in 2024.

SECTION 2 • THE FOUNDATION

FCI, CUI, and FAR 52.204-21

The requirements every federal contractor already has — and the distinction that drives everything else.



Two Categories, Two Very Different Requirements

Federal Contract Information (FCI)

What it is: Information provided by or generated for the government under a contract that is not intended for public release

Examples: Contract terms, delivery schedules, technical drawings (unclassified), internal project communications

Baseline rule: FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems) - 15 basic requirements

Applies to: Nearly every federal contract - this is the floor for everyone

Controlled Unclassified Information (CUI)

What it is: Information the government (or a contractor on its behalf) creates or possesses that requires safeguarding under a law, regulation, or government-wide policy

Examples: Export-controlled data, procurement-sensitive info, PII in federal programs, critical infrastructure info, health/law-enforcement data

Baseline rule: NIST SP 800-171 (currently Rev 2 for CMMC; Rev 3 for GSA and forthcoming FAR CUI rule)

Applies to: Only contracts where CUI is actually involved — identified by the contracting agency

Basic Safeguarding: The 15 Requirements Every Federal Contractor Has

KEY IDEA

If you have any federal contract, FAR 52.204-21 already applies. These 15 requirements are derived from NIST SP 800-171 and represent the minimum. They apply whether you handle CUI or not.

1**Identity and access control (7 requirements)**

Limit system access to authorized users; verify identities; limit and enforce authorized functions; sanitize media; control physical access; escort/monitor visitors; maintain audit logs

2**System boundary protection (2 requirements)**

Monitor, control, and protect communications at external boundaries; implement subnetworks for publicly accessible components

3**Identification and authentication (2 requirements)**

Identify users; authenticate before granting access

4**Media and physical protection (2 requirements)**

Sanitize or destroy media before disposal; control physical access to information systems

5**System and information integrity (2 requirements)**

Identify and correct system flaws in a timely manner; provide protection from malicious code

How to Know What Applies to a Specific Contract



1. Look for FAR 52.204-21

- Present in nearly every federal contract
- If it's there, the 15 basic safeguarding requirements apply
- Flow-down to subcontractors is required



2. Look for DFARS 252.204-7012

- DoD contracts (and DoW-supply-chain flow-downs)
- Triggers NIST 800-171 requirements + cyber incident reporting
- May trigger CMMC L2 assessment obligations



3. Look for the new SF XXX (coming)

- Under the forthcoming FAR CUI rule - Standard Form XXX
- Identifies whether CUI is involved and what handling applies
- Look for FAR 52.240-6 and 52.240-7 clauses



4. Look for agency-specific clauses

- GSA: reference to CIO-IT Security-21-112 procedural guide
- HHS: HIPAA business associate language
- Treasury, DHS, DOE, others: agency-specific security requirements

SECTION 3 • GSA CUI FRAMEWORK

GSA's January 2026 Procedural Guide

The first major civilian framework - CMMC-like, but stricter in several ways.



The IT Security Procedural Guide (CIO-IT Security-21-112 Rev 1)

WHAT HAPPENED

On January 5, 2026, GSA released Revision 1 of its IT Security Procedural Guide titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Process." The guide creates a CMMC-like framework for GSA contractors handling CUI but with several notable differences from the DoW's CMMC program.

NIST 800-171

Revision 3

*Not Rev 2 like CMMC — 97 requirements,
aligned with 800-53 Rev 5*

3rd-Party

Assessment

*FedRAMP 3PAO or GSA-approved assessor
with no self-attestation*

1-Hour

Reporting

*Suspected or confirmed CUI incidents
The tightest in federal contracting*

5-Phase

Lifecycle

*Prepare · Document · Assess · Authorize ·
Monitor*

The Nine Showstopper Controls

KEY IDEA

Showstopper controls are pre-approval requirements that must be fully implemented before GSA will authorize a contractor's system. There is no room to defer these to a Plan of Action and Milestones.

1**Multi-factor authentication (phishing-resistant)**

Required for privileged access, remote access, and network access to non-privileged accounts

2**Boundary isolation of the CUI environment**

CUI environment must be isolated from corporate networks; jump servers with MFA for remote access

3**Cryptographic protection of CUI**

FIPS-validated encryption for CUI at rest and in transit. Not just "encryption" in general

4**Continuous vulnerability scanning**

Ongoing scanning tied to CISA Binding Operational Directives and Known Exploited Vulnerabilities

5**Replacement of unsupported system components**

End-of-life software and hardware cannot remain in the CUI environment

6**Secure remote access controls**

Approved, monitored, encrypted remote access mechanisms only

7**Incident response capability with 1-hour reporting**

Suspected or confirmed CUI incidents reported to GSA within one hour of discovery

NIST SP 800-171 Rev 3 vs. Rev 2

Rev 2 (still the CMMC baseline)

Requirements: 110 base requirements across 14 control families

Assessment objectives: 320 assessment objectives (from NIST SP 800-171A)

ODPs: No organization-defined parameters. All requirements are fixed

Alignment: Based on the earlier version of NIST SP 800-53

Where required: CMMC (DoW contracts); most current DFARS references

Rev 3 (GSA baseline; coming FAR CUI baseline)

Requirements: 97 base requirements across 17 control families (3 new: Planning, System & Services Acquisition, Supply Chain Risk Mgmt)

Assessment objectives: More objectives per requirement with broader security scope and higher bar

ODPs: Introduces organization-defined parameters. You must document values for frequencies, thresholds, and types

Alignment: Aligned with the current NIST SP 800-53 Rev 5

Where required: GSA CUI framework; forthcoming FAR CUI rule; likely future civilian agency adoption

The Substantive Differences Between Rev 2 and Rev 3



Three New Control Families

- Planning (PL) — formalizes the SSP and rules of behavior (implicit in Rev 2, explicit now)
- System and Services Acquisition (SA) — secure development and external service providers
- Supply Chain Risk Management (SR) — the biggest addition, driven by SolarWinds-era attacks



Organization-Defined Parameters (ODPs)

- 88 ODPs introduced — bracketed placeholders where you specify the value
- Replaces vague language like "periodically" with concrete, documented values
- You define the frequency, threshold, or type — and defend that definition



No More "NFO" Hidden Controls

- Rev 2 assumed 60+ Non-Federal Organization (NFO) controls were in place
- These were a top cause of failed CMMC assessments — nobody knew they applied
- Rev 3 removes NFOs entirely; if it's not in the requirements, it's not required



Cleaner Structure, Stricter Wording

- No more "basic vs. derived" distinction — 800-53 is the single authoritative source
- 70+ requirements got wording updates for precision and clarity
- Some requirements got stricter — e.g., 3.4.8 now allow-listing only, not deny-listing

What the Rev 2 → Rev 3 Shift Means Practically

THE BIG IDEA

Fewer controls doesn't mean less work. The assessment burden grew, the documentation load grew, and organizations with a Rev 2 SSP will need to do real work to move to Rev 3.

1

MORE ASSESSMENT WORK

Verification Load Grew

422 determination statements plus 88 ODPs to specify — over 500 items to document. The lower control count is misleading; the assessment burden is heavier, not lighter.

2

MORE DOCUMENTATION

ODPs Are Real Work

Every ODP is a policy decision you must document, defend, and consistently apply. Frequencies, thresholds, and types that Rev 2 left implicit now have to be written down and enforced.

3

CROSSWALK REQUIRED

Your Rev 2 SSP Won't Just Convert

The families reorganized, controls consolidated, and numbering changed. Anyone with existing Rev 2 documentation needs to build a crosswalk — control-by-control — to identify what maps, what's new, and what got stricter.

BOTTOM LINE

Start early: if you're likely to face Rev 3 through GSA or the coming FAR CUI rule, begin the crosswalk now. Waiting until a contract requires it is waiting too long.

SECTION 4 • THE FAR CUI RULE

The June 2026 Revised Proposed Rule

The government-wide standardization that will change every civilian federal contract.

The FAR CUI Rule at a Glance



Standardizes Government-Wide

- Replaces agency-by-agency CUI patchwork with one uniform framework
- Applies across federal executive branch, both defense and civilian
- Consolidates CUI provisions in new FAR Part 40 (Information Security and Supply Chain Security)



Introduces Standard Form XXX

- Contracting officers complete SF XXX to identify CUI in each contract
- Specifies CUI categories, safeguarding, marking, and reporting requirements
- Uniform disclosure vehicle attached to solicitations and contracts



New Clauses 52.240-6 and 52.240-7

- 52.240-6: Solicitation provision - Notice of CUI requirements
- 52.240-7: Contract clause - Substantive CUI safeguarding and reporting
- Flow-down to subcontractors that will handle CUI



Requires NIST 800-171 Rev 3

- Contractors self-attest compliance with Rev 3 (not third-party like GSA/CMMC)
- Applies to contractor information systems that handle CUI
- Includes commercial products/services - except COTS

Timeline, Reporting, and What Comes Next

RULE-MAKING TIMELINE



KEY DETAILS FROM THE JUNE 2026 REVISED RULE

72-hour incident reporting Suspected or confirmed CUI incidents reported within 72 hours of discovery - matches DFARS timing
No implementation phase-in Once final, clauses go into new contracts immediately - no ramp-up period like CMMC had
Applies to commercial products/services (except COTS) Commercial and non-commercial procurements alike; only commercial off-the-shelf items are excluded
Subcontractor flow-down required Requirements pass to subs that will handle CUI - primes must include and enforce

What Non-DoW Contractors Should Prepare For Now



Identify Where CUI May Land

- Inventory what federal contracts you hold - direct and subcontract
- Look for CUI markings, sensitive data handling clauses, and agency-specific security terms
- Even if you're not a prime, a flow-down clause can bring CUI to you



Start Reading Rev 3

- The FAR CUI rule requires Rev 3, not Rev 2
- Rev 3 has fewer requirements (97 vs 110) but a broader scope and organization-defined parameters
- Free NIST resources and mapping tools available



Get the SSP Started

- A System Security Plan is required - it describes how you meet each requirement
- Reflects actual practice, not aspirational - including external providers
- Assessors and contracting officers will ask to see it



Assign Clear Ownership

- Assign accountability across IT, contracts, and operations
- These obligations tend to fall through gaps when no single person owns them
- Executives may bear individual responsibilities under the rule

SECTION 5 • OTHER REQUIREMENTS

Sector Rules, State Laws, and Insurance

Federal contracting rules aren't the only cybersecurity requirements Wisconsin businesses face.



Federal Sector-Specific Cybersecurity Rules



FTC Safeguards Rule

- Applies to "financial institutions" (broadly defined - includes tax preparers, mortgage brokers, auto dealers)
- Requires a written information security program with specific elements
- Reach expanded significantly in the 2021-2023 amendments - many businesses that never thought of themselves as "financial" are now covered



HIPAA & HITECH

- Applies to covered entities and business associates handling protected health information (PHI)
- Business Associates: IT vendors, billing services, contractors serving healthcare - the rules follow the data
- Specific administrative, physical, and technical safeguards required



PCI-DSS

- Applies to any business that stores, processes, or transmits credit card data
- Required by card networks and processors - not by federal law
- Failure can mean fines, higher processing fees, or loss of ability to accept cards



GLBA – Gramm-Leach-Bliley Act

- Applies to banks, credit unions, insurance companies, and some financial services firms
- Requires a written information security program and safeguards for customer information
- Overlaps with FTC Safeguards Rule for many businesses

Wisconsin and Multi-State Data Protection Laws

KEY IDEA

Even without federal contracts, most Wisconsin businesses already have state cybersecurity obligations — and if you have customers outside Wisconsin, other states' laws apply too.

1

Wisconsin Statute § 134.98 — Notice of Unauthorized Acquisition of Personal Information

If personal information of a Wisconsin resident is acquired by an unauthorized person, notification is required within 45 days. Applies to nearly any business with WI customer data

2

Other states' breach notification laws apply based on where customers live

All 50 states have breach notification laws with varying triggers, timelines, and penalties. California, New York, Illinois, and Massachusetts have some of the strictest

3

State-specific privacy laws are expanding

California (CCPA/CPRA), Virginia, Colorado, Connecticut, and others impose consumer privacy obligations on out-of-state businesses serving their residents. More states are joining every year

4

Wisconsin sector rules apply on top

Wisconsin DFI rules for financial data, DHS for health information, DOR for tax preparers - sector matters even at the state level

Cybersecurity Insurance: The Third Set of Requirements

What Carriers Are Requiring

MFA everywhere: Multi-factor authentication on email, remote access, and administrative accounts - table stakes for most carriers now

Documented backups: Tested backup process with off-site or immutable copies; regular restore testing

Endpoint protection: Antivirus or EDR on every business system, kept updated

Patch management: Documented process for applying security updates within defined timeframes

Awareness training: Annual security training for employees, with completion records

Common Reasons Claims Get Denied

Misrepresentation: Application said you had MFA but you didn't - insurers can deny for material misrepresentation on the application

Pre-existing incident: Attacker was in your network before the policy started (even unknowingly) - coverage often excluded

Excluded scenarios: Wire fraud, social engineering, and "act of war" exclusions are increasingly broad in policies

Notification failures: Failed to notify the carrier within the policy's required window - common technical basis for denial

Control decay: Controls that existed at application no longer functioning at time of claim

SECTION 6 • DECISION FRAMEWORK

What Actually Applies to You?



The Three Questions That Drive Your Requirements

THE BIG IDEA

You don't need a lawyer or a compliance consultant to begin to identify your starting requirements. Working through these three questions honestly will identify the vast majority of what applies.

1

QUESTION 1

What Data Do You Have?

Federal contract information? FAR 52.204-21. CUI? NIST 800-171 (Rev 2 or Rev 3, depending on the agency). Credit cards? PCI-DSS. Health data? HIPAA. Financial data on individuals? FTC Safeguards or GLBA. Personal data of any resident? State breach laws.

2

QUESTION 2

Who Are Your Customers?

Federal government? FAR baseline plus agency-specific rules - GSA has its own now. State or local government? Increasingly common cybersecurity clauses in procurement. Federal prime contractors? Flow-down requirements can bring surprising obligations to subs. Consumers in specific states? Those states' laws apply.

3

QUESTION 3

What Do Your Contracts Say?

Contract language is where the most specific obligations actually live — often more specific than the underlying regulations. Read the security, confidentiality, and incident-response clauses in every federal contract, prime-sub agreement, and cybersecurity insurance policy you hold.

BOTTOM LINE

Document your answers in a one-page summary. That summary becomes your kick off to a compliance roadmap and the basis for everything else.

Walking a Typical Wisconsin Business Through the Framework

SCENARIO

A Milwaukee-area precision machining company (25 employees) supplies parts to a large civilian federal prime contractor. They also do commercial work for local manufacturers. No DoW work directly. They handle drawings and specifications from the prime.

Question 1 — What Data Do They Have?

Prime provides drawings marked with CUI handling instructions (export-controlled technical data). No credit card processing. Standard payroll data on employees only. No customer health data.

→ CUI applies. Rev 2 or Rev 3 depending on the prime's flow-down. State breach law applies to employee PII.

Question 2 — Who Are Their Customers?

Federal civilian prime contractor (flow-down). Wisconsin manufacturers (commercial). No direct federal contracts held today, but that could change.

→ FAR 52.204-21 flows down. If the prime is under the coming FAR CUI rule, those flow-downs come too. GSA rules could apply if they win a GSA schedule contract.

Question 3 — What Do Their Contracts Say?

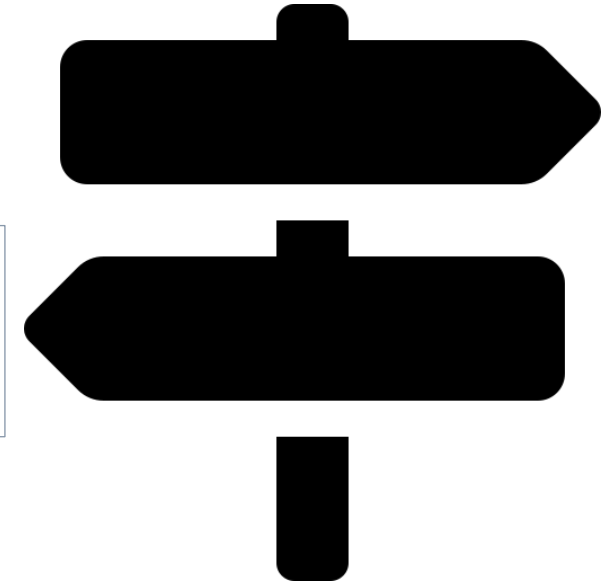
Prime contract includes: FAR 52.204-21, DFARS-style handling for CUI drawings, incident notification within 72 hours, right-to-audit clause. Cyber insurance policy requires MFA and documented backups.

→ Contract-level obligations are the binding minimum. The cyber insurance requirements are a separate but overlapping set. Both must be met.

SECTION 7 • GETTING READY

Practical Starting Points

Where to begin, no matter where your business is today.



Where to Start Based on Where You Land

Not everyone needs to solve the same problem. Match your starting point to where you actually are.

IF YOU HAVE No federal contracts yet	IF YOU HAVE FAR 52.204-21 (baseline)	IF YOU HAVE CUI from any agency	IF YOU HAVE GSA contracts with CUI
• Start with FAR 52.204-21 as a preview of the baseline • Get the security basics right: MFA, backups, patches, awareness • Review cyber insurance and state breach law obligations	• Confirm all 15 basic safeguarding requirements are actually met • Document what you have in a SSP-style summary • Watch for CUI flow-downs from primes	• Confirm which NIST 800-171 revision applies (2 or 3) • Build or update your SSP; identify gaps and POA&Ms • Prepare for third-party assessment if GSA - self-attest if FAR CUI	• Assess against Rev 3 immediately - start gap analysis • Address the nine showstoppers first - no POA&M option • Engage a 3PAO early - assessment backlogs are already forming

COMMON THREAD: *Regardless of where you start, get your inventory, MFA, backups, and documented policies in place first. Everything else builds on that foundation.*

Where to Get Help

You don't have to figure this out alone - free federal, state, and Wisconsin resources exist for exactly this.

Wisconsin Procurement Institute (WPI)

wispro.org

Free consulting for Wisconsin businesses navigating federal cybersecurity and contracting requirements

CISA Cyber Essentials

cisa.gov/cyber-essentials

Federal government's free starter framework - six concrete actions every leader can take

NIST 800-171 Rev 3 Publication

csrc.nist.gov/publications

The current baseline for GSA CUI framework and the coming FAR CUI rule - free from NIST

GSA IT Security Procedural Guide

gsa.gov/technology (search CIO-IT Security-21-112)

The full text of GSA's January 2026 CUI framework document - the source of the showstopper requirements

Federal Register - FAR CUI Rule

federalregister.gov (search FAR Case 2026-001)

The June 2026 revised proposed rule - full text and public comments received

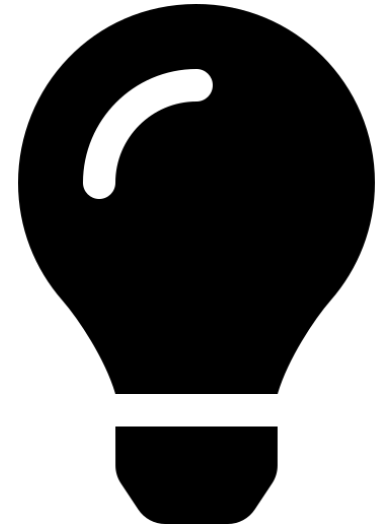
Wisconsin DATCP - Consumer Protection

datcp.wi.gov

Wisconsin breach notification guidance, identity theft resources, and small business protection

Key Takeaways

- Non-DoW cybersecurity requirements changed more in the last 18 months than the previous decade - GSA's January 2026 framework and the June 2026 revised FAR CUI rule are the big ones
- The distinction between FCI and CUI drives everything else - FCI triggers FAR 52.204-21's 15 basic requirements; CUI triggers NIST 800-171 (Rev 2 or Rev 3 depending on agency)
- GSA is the first major civilian framework - Rev 3 baseline, third-party assessment, nine showstoppers, and one-hour incident reporting; no transition period
- The FAR CUI rule will standardize CUI protection across the federal government - new FAR Part 40, Standard Form XXX, clauses 52.240-6 and 52.240-7, Rev 3 controls, 72-hour reporting
- Federal rules are not your only cybersecurity requirements - sector rules (FTC Safeguards, HIPAA, PCI-DSS), Wisconsin § 134.98, and cyber insurance obligations often overlap
- The three-question framework - what data, what customers, what contracts - gets you most of the way to a defensible view of what applies to your business



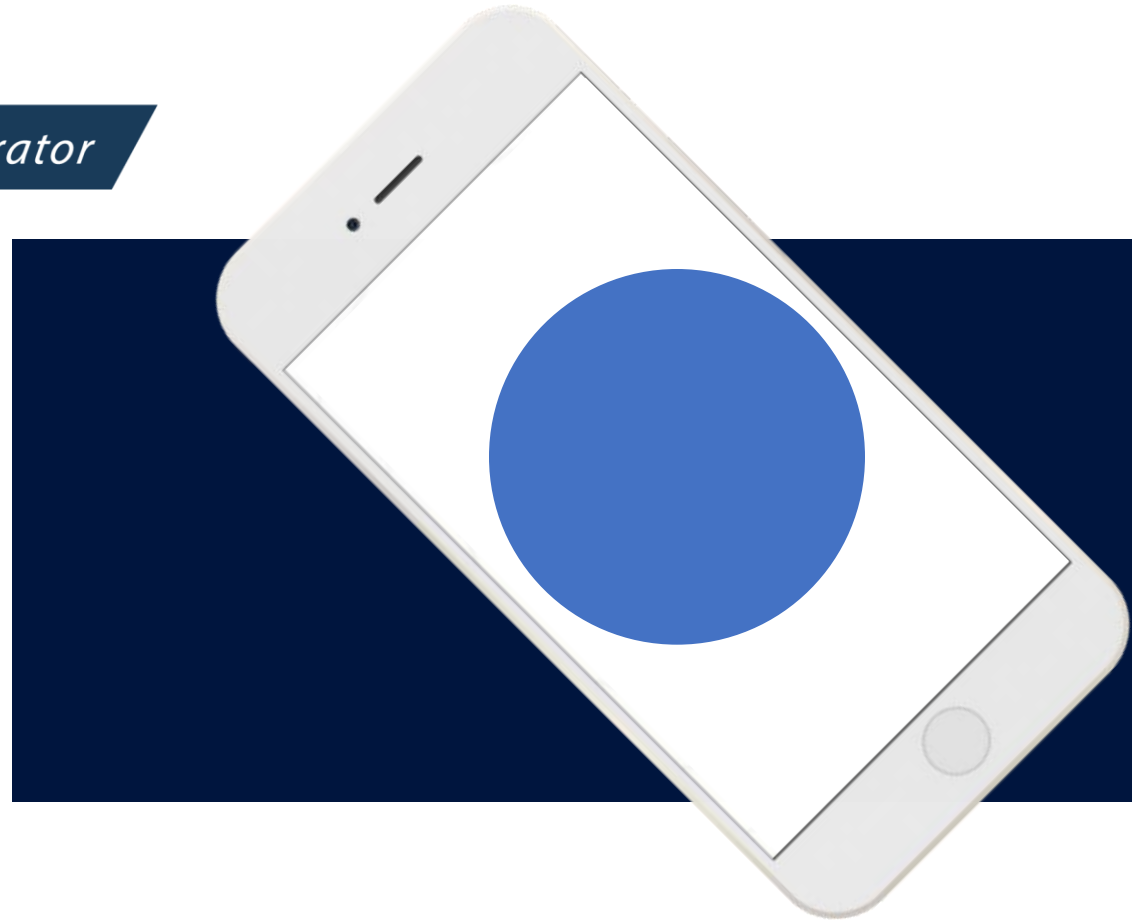
ONE THING TO DO THIS WEEK: *Pull one federal contract off the shelf and read its cybersecurity clauses end-to-end. You'll be surprised what's in there.*



An APEX Accelerator

Matthew Frost

mattf@wispro.org



Upcoming Events



Cyber Thursday

Cyber Thursday 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.

- July 9 – Cybersecurity Requirements for Non-Department of War Contractors and Suppliers
- July 16 – A Guide to Strong Supporting Documentation
- August 27 – Determining Your Real CMMC Compliance Responsibilities

...More information and registrations at wispro.org/events

Federal Market Insights

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

- June 23 – Understanding Sealift
- June 30 – Issues Facing the DIB

...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

**This webinar is eligible for
1 CPE credit**

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

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MattF@wispro.org | 414-270-3600

10437 W. Innovation Drive Suite 253
Milwaukee WI 53226