

Cyber Thursday:

A Guide to Strong Supporting Documentation

July 16 | 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**

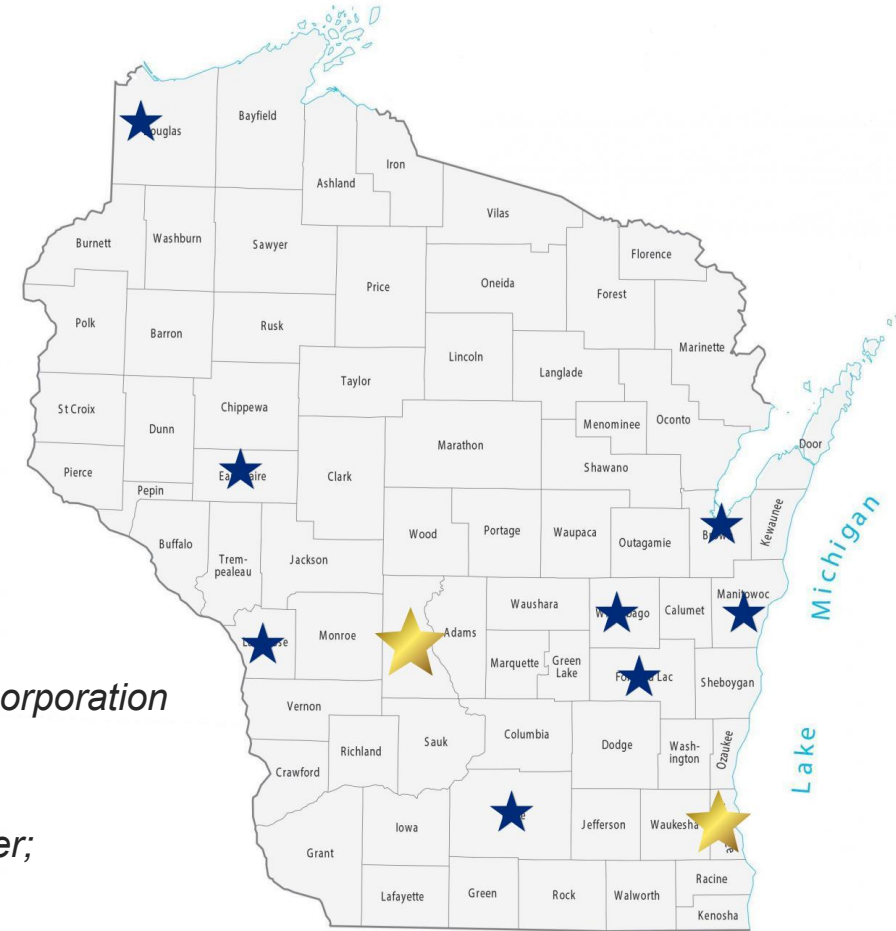
- *Progress Lakeshore*

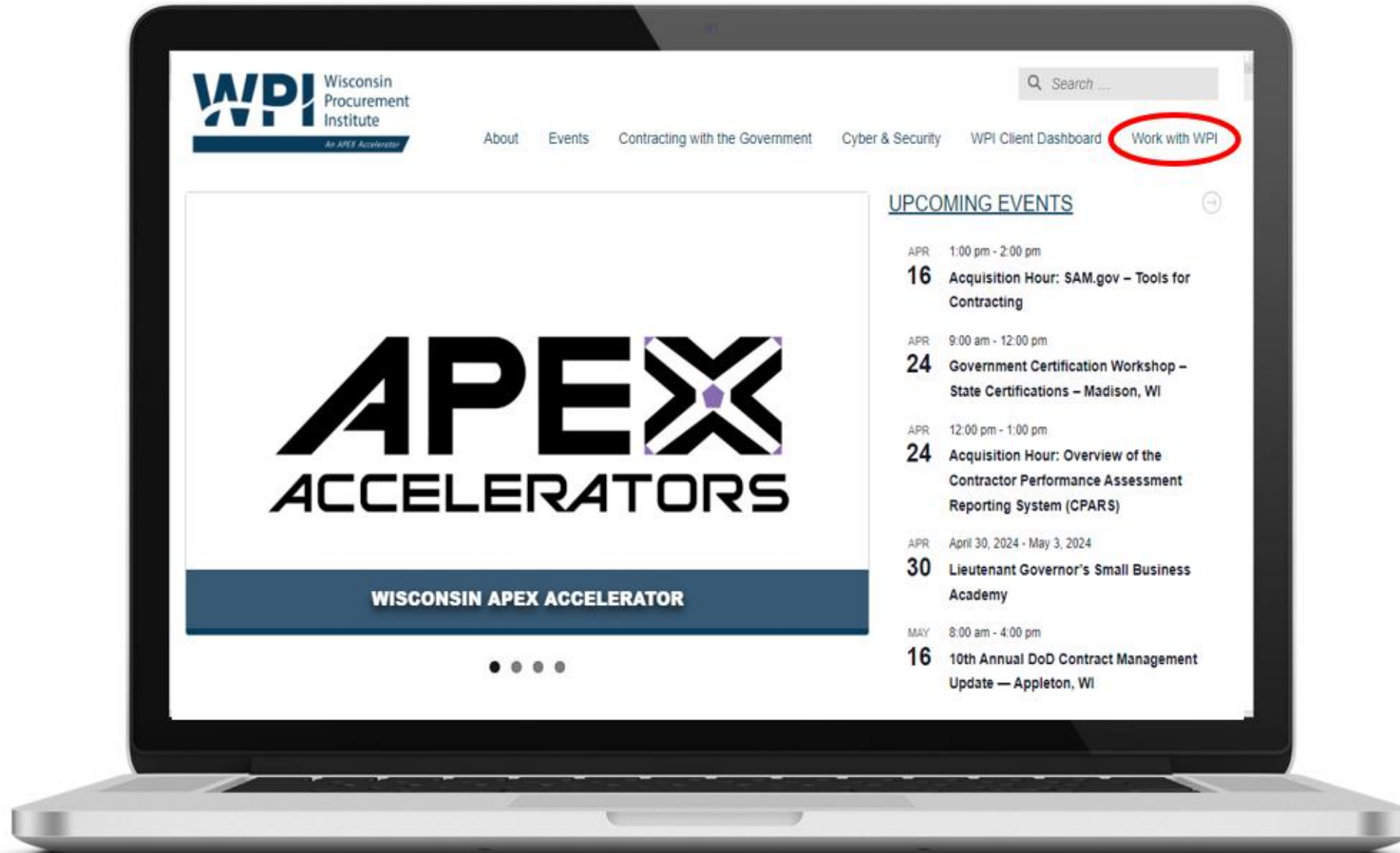
- **OSHKOSH**

- *Greater Oshkosh
Economic Development Corporation*

- **SUPERIOR**

- *Small Business Dev Center;
UW Superior*

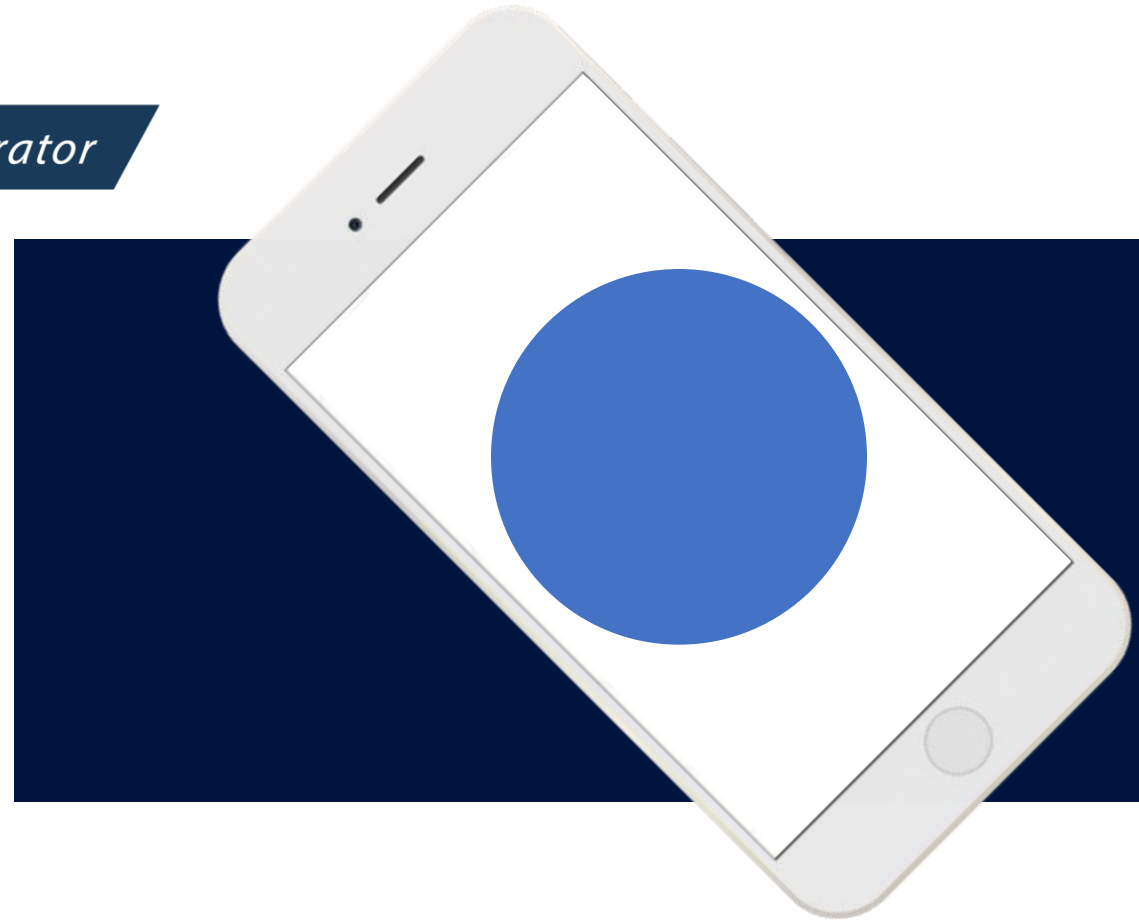






An APEX Accelerator

A Guide to Strong Supporting Documentation



Cyber Thursday – July 16th, 2026

**BUT WAIT – THERE IS BIG
NEWS**

The Headline — and Why It Matters

JULY 13, 2026

The Department of War immediately suspended CMMC Phase II — the third-party assessment requirement that was scheduled to take effect November 10, 2026.

WHAT'S EASY TO MISREAD

This is not "CMMC is dead."

The DoW suspended one specific phase of implementation — third-party (C3PAO) assessment. CMMC as a program remains codified in 48 CFR. Phase I self-assessments are still required

This is not "we can stop preparing."

DFARS 252.204-7012 and NIST SP 800-171 Rev 2 still apply. DIBCAC can still assess. False Claims Act liability is unchanged. Cybersecurity obligations for handling CUI have not moved

This is not "cybersecurity requirements were reduced."

In the CIO's own words: "We are not reducing cybersecurity through this measure. We are reducing the red tape." What changed is who checks your work — not what the work is

Why the DoW Says They Did This

KEY IDEA

The memo cites specific concerns from Small Business Administration data and industry feedback. Understanding the reasoning helps predict what the Task Force may recommend.

1**Prohibitive compliance costs on small and mid-sized businesses**

The memo cites SBA estimates exceeding \$7 billion per year in aggregate compliance costs for the DIB — cited as a barrier forcing innovative businesses out of the market

2**Severe shortages in third-party assessment capacity**

The DoW pointed to over 100,000 DIB businesses needing assessment against roughly 100 authorized C3PAOs — a math problem the CIO called "simply not mathing"

3**Structural incompatibility with acquisition reform**

The memo argues that CMMC "as currently planned" conflicts with Hegseth's Acquisition Transformation Strategy focus on speed to capability and removing bureaucratic barriers

4**Impact on commercial and nontraditional companies**

SBA data suggested CMMC was pushing innovative new entrants out of defense contracts, at a time when the DoW says it urgently needs their capabilities

What the July 13 Memo Says

Who Signed It

- DoW CIO Kirsten Davies (author of the memo)
- Under Secretary of War for Acquisition and Sustainment Michael Duffey
- In support of Secretary of War Pete Hegseth's Acquisition Transformation Strategy
- Memo dated July 10, publicly announced July 13



What Contracting Officers Must Do

- Amend active solicitations that contain Level 2 (C3PAO) or Level 3 requirements
- Modify existing contracts with those requirements at the next option or scheduled modification
- Only include Level 1 (Self) or Level 2 (Self) in new procurement requests
- May not designate Level 2 (C3PAO) or Level 3 during the review period



What It Suspends

- CMMC Phase II — the C3PAO assessment requirement for Level 2
- Phase III — the DIBCAC assessment requirement for Level 3
- All pending and future CMMC implementation milestones "until further notice"
- CMMC waiver procedures pending the 60-day review



What's Next

- 60-day CMMC Reform Task Force — report due on or about September 13, 2026
- Request for Information (RFI) open for public comment through Aug 14, 2026
- Cross-functional team from CIO, Acquisition, R&E, Legal, and other directorates
- Outcome could be reform, delay, restructuring, or (they haven't ruled out) cancellation

What's Suspended vs. What's Still in Force

What IS Suspended

Phase II C3PAO requirement: The Nov 10, 2026 transition to third-party assessment for Level 2 is on hold indefinitely

Phase III DIBCAC requirement: The Nov 10, 2027 rollout of government-led Level 3 assessments is also on hold

Active solicitation requirements: Current solicitations with Level 2 (C3PAO) or Level 3 language must be amended to remove them

Waiver procedures: CMMC waiver processes are paused pending the review

New CMMC designations: Contracting officers may not designate Level 2 (C3PAO) or Level 3 during the review

What IS Still in Force

Phase I self-assessments: Level 1 (Self) and Level 2 (Self) requirements remain firmly in place with annual affirmations

DFARS 252.204-7012: Safeguarding covered defense information and cyber incident reporting unchanged

NIST SP 800-171 Rev 2: Baseline for CUI protection is unchanged — all 110 requirements still apply

SPRS scoring: Level 2 minimum score of 88/110 still required for self-assessed contracts

DIBCAC & False Claims Act: DIBCAC can still audit; FCA liability for cybersecurity claims continues (LOGZONE settled for \$507K in June 2026)

Back to our program.

Documentation Is the Assessment

The Rule

Assessors don't give credit for controls they can't verify.

WHAT THIS ACTUALLY MEANS

A well-implemented control with weak documentation fails.

You may actually be doing the right thing but if you can't show the policy, the procedure, and the evidence, the assessor cannot mark the objective as MET

A well-documented control with modest implementation likely has a better opportunity to pass.

Not because documentation replaces implementation, but because "MET" is defined by evidence. Clear policies, working procedures, and current artifacts satisfy the standard

Every hour spent on documentation saves five during the assessment.

The C3PAO is on the clock. If evidence isn't organized and retrievable in seconds, you burn assessment hours you're paying for and lose the assessor's trust

What We'll Cover

1

The Documentation Landscape

What documents CMMC L2 actually expects, and the three-tier model

2

Policies and Procedures

The building blocks what each one is, what each one contains

3

Evidence Artifacts

Screenshots, configs, logs, tickets - what counts and how to organize it

4

Shared Responsibility

Cloud providers, MSPs, and who is responsible for which control

5

The System Security Plan

The master document that pulls everything together

6

The Plan of Action and Milestones

How you track and remediate what's not yet in place

7

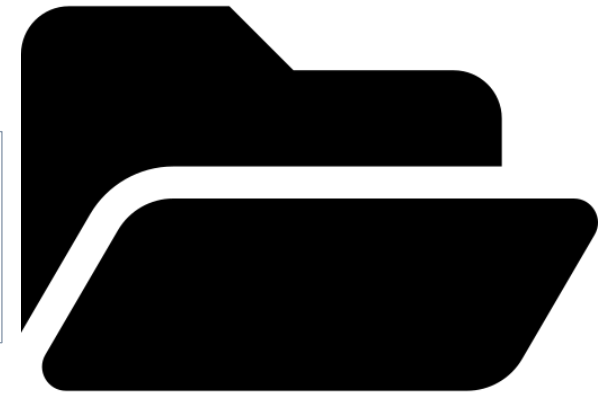
Putting It Together

How the package works as one coherent story for an assessor

SECTION 1 • THE DOCUMENTATION LANDSCAPE

The Documentation Family

Before you can build it, you need to know what "it" actually is.



The Documents CMMC L2 Actually Expects to See

KEY IDEA

CMMC L2 doesn't require a single document — it requires an interlocking set of them. Every one of these has a role in the assessment; missing any one creates gaps that map directly to objectives not MET.

1**System Security Plan (SSP)**

The master document — describes your CUI environment, boundary, and how each of the 110 controls is implemented

2**Plan of Action and Milestones (POA&M)**

The register of unmet or partially-met requirements with dated remediation plans and owners

3**Policies (one per control family, or a master)**

"What we do" — high-level, leadership-approved statements of how the organization addresses each control family

4**Procedures (per policy or per process)**

"How we do it" — the step-by-step operational detail that translates policy into daily action

5**Evidence artifacts (per control)**

"Proof we did it" — screenshots, configs, logs, tickets, training records, meeting minutes, scan reports

6**Shared Responsibility Matrix / CRM**

For every cloud provider and MSP in your CUI environment — who owns each control, who inherits, who configures

7**Standalone plans (IR, DR, CM, Incident Response)**

Several controls explicitly require named plans — Incident Response Plan, Configuration Management Plan, and others

Policy • Procedure • Evidence: The Three Tiers Every Control Needs

THE BIG IDEA

Every one of the 110 CMMC L2 controls needs all three tiers behind it. Missing any tier — even for a control you meet in practice — is how well-run organizations end up with objectives not MET.

1

TIER 1 — POLICY

What We Do

High-level, leadership-approved statement of the organization's position. Establishes authority, scope, and roles. Answers "we do this because our policy says so." Signed, dated, and reviewed on a documented cadence.

2

TIER 2 — PROCEDURE

How We Do It

The step-by-step operational detail that turns policy into action. Names the tools, the people, the steps, and the frequency. Answers "here's exactly what happens." Owned by the team that runs the process.

3

TIER 3 — EVIDENCE

Proof We Did It

The artifacts that show the procedure actually ran — screenshots, logs, tickets, training records, scan output, meeting minutes. Answers "here's what happened on this specific date." Current, dated, and retrievable.

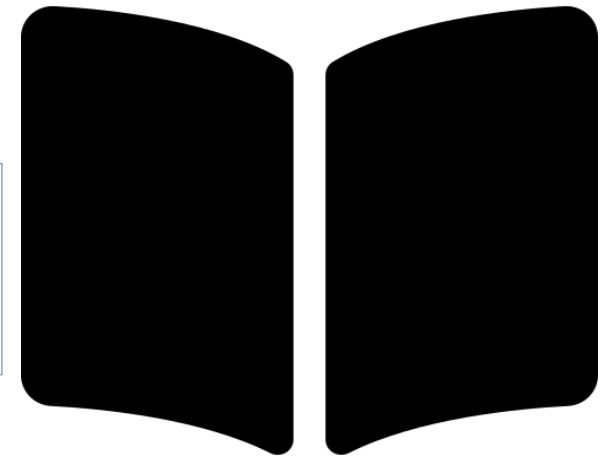
BOTTOM LINE

A control statement without all three tiers is a control an assessor cannot verify. This model is the mental checklist for every documentation decision you make.

SECTION 2 • POLICIES AND PROCEDURES

Policies and Procedures

The building blocks — what each one is, what each one contains, and why assessors care about the difference.



Policy vs. Procedure: What Each Actually Is

Policy

Purpose: States the organization's position, authority, and expectations for a control family or topic area

Audience: All employees, leadership, external parties — anyone who needs to know "why we do this"

Length: Usually 1-3 pages per family; concise and high-level

Owner: Leadership (CEO, CISO, or delegated policy authority) — must be approved at the executive level

Update cadence: Reviewed annually at minimum; updated on material change; version-controlled and dated

Sample content: Scope, roles and responsibilities, high-level requirements, exceptions process, enforcement

Procedure

Purpose: Describes the operational steps to implement the policy — the actual actions taken to satisfy the control

Audience: The people who perform the work — sysadmins, security team, help desk, operations

Length: As long as needed for clarity; often multiple procedures per policy

Owner: The operational team that runs the process — must be accurate to how the work actually happens

Update cadence: Updated when tools, processes, or people change; reviewed at least annually

Sample content: Step-by-step actions, tools used, frequency, approvals required, escalation paths, sample outputs

Structuring Policies for CMMC L2



Option A: One Policy Per Family

- 14 discrete policies — one for each control family (AC, AT, AU, CM, etc.)
- Easier to align with the assessment (assessors know which policy to ask for)
- Best for organizations with dedicated compliance staff or policy libraries



Option B: Master Policy Document

- One integrated cybersecurity policy with sections for each family
- Easier to maintain (one review cycle, one approval)
- Best for smaller organizations without a policy program



Either Way: Required Elements

- Approval signature and date from leadership authority
- Version number and revision history
- Defined scope, roles, and enforcement
- Reference to which controls the policy addresses



Common Failure Modes

- Template policies never customized to your organization
- Policies signed years ago and never re-approved
- Policies that don't reference the actual environment or systems
- Aspirational policies that describe what you'll do someday, not what you do

Writing Procedures That Assessors Accept

KEY IDEA

A procedure isn't a checklist — it's a documented process that a new employee could follow and get the same result as your senior sysadmin. It must be accurate to how the work is done, not to how you wish it were done.

1**Name the tool, not the category**

Not "use a vulnerability scanner" — "run Tenable Nessus with policy X against subnet Y every 30 days." Assessors verify the specific tool exists and produces the expected output

2**Name the role or role, not the person**

"The Security Analyst reviews logs weekly" — not "Bob reviews logs weekly." People change; roles persist. But the role must exist in the org chart

3**State frequency in the procedure, not "as needed"**

"Monthly on the first Tuesday" beats "periodically" or "as needed." Assessors will ask when this was last done — the procedure needs to define the answer

4**Include approvals and escalations**

Who approves? Who gets called when it doesn't go as planned? Procedures that go silent at decision points are procedures that don't hold up under scrutiny

5**Reference the artifacts the procedure produces**

"...and the results are saved to \\evidence\vuln-scans\YYYY-MM." This creates the evidence trail before the assessment even starts

SECTION 3 • EVIDENCE ARTIFACTS

Evidence Artifacts

The proof that turns "we have a policy" into "we actually do this."

What Counts as Evidence



System-Generated Output

- Screenshots of configuration settings with timestamps and system context
- Exported reports from your SIEM, MDM, EDR, patch management tools
- Scan results (vulnerability scans, configuration compliance scans)
- Log excerpts showing the control operating



Process Records

- Change tickets showing review, approval, and implementation
- Access request/approval forms (physical and logical)
- Incident tickets with response timelines
- Meeting minutes for security review meetings or risk assessments



Personnel Records

- Training completion records (name, date, course, score if applicable)
- Acknowledgment of policies and acceptable use
- Background check completion records
- Onboarding/offboarding checklists showing access provisioning/revocation



Governance Artifacts

- Signed and dated policies and procedures
- Risk assessment reports
- Third-party assessment results (penetration tests, audits)
- Executive review sign-offs on the SSP and POA&M

Organizing Evidence for an Assessment

KEY IDEA

The C3PAO is on the clock. Evidence that isn't organized, current, and retrievable in under a minute is evidence that costs you assessment time and assessor confidence. Organization matters as much as content.

1**Build an evidence library indexed by control**

One folder per control (or per objective). File names carry date, system, and type. Assessors follow the SSP into the library — the mapping must be obvious

2**Standardize naming conventions**

YYYY-MM-DD_<system>_<artifact-type>_<control-id>.<ext>. The name alone should tell an assessor what they're looking at

3**Verify currency — evidence expires**

Evidence from three years ago rarely counts. Most evidence should be within the last 90 days to 12 months, depending on the control's cadence

4**Map every objective to at least one artifact**

For each of the 320 assessment objectives, name the evidence that satisfies it. The mapping IS the deliverable, not an afterthought

5**Store evidence separately from the systems it describes**

If your evidence lives only on the system being assessed, a compromise of that system can eliminate your evidence. Off-system, backed-up storage is the standard

The "Show Me" Test

THE BIG IDEA

For every one of the 110 controls, can you produce the requested evidence within a minute? If not, your evidence isn't ready for an assessment — regardless of whether it exists somewhere.

1

TEST 1

Named and Locatable

The assessor names a control. You can go directly to its evidence folder without hesitation. Nobody says "let me find that" or "I think Bob has it." Location is documented, not tribal knowledge.

2

TEST 2

Current and Dated

The evidence you retrieve is from within the appropriate window for the control. Nothing is undated. Nothing predates the last review cycle. Evidence expiration is tracked as actively as the evidence itself.

3

TEST 3

Complete and Traceable

The evidence satisfies every objective for that control — not just "an artifact exists." It maps to the SSP implementation statement, the procedure that produced it, and the policy that authorizes it.

BOTTOM LINE

If all three tests pass for every control, you are documentation-ready. If any fails on any control, that's your next work item — before assessment day.

SECTION 4 • SHARED RESPONSIBILITY

Shared Responsibility



The cloud and MSP question that quietly wrecks unprepared assessments.

You Don't Own Every Control — But You're Responsible For All of Them

THE REALITY

Nearly every CMMC L2 environment involves external providers — Microsoft 365 GCC High, Azure Government, AWS GovCloud, MSPs, MSSPs, backup providers. You cannot delegate CMMC responsibility to them, but you can (and must) delegate specific controls. The documentation must show which controls YOU perform, which they perform, and which are shared.

HOW THIS GOES WRONG

"Our MSP handles that."

The contractor assumes the MSP owns a control; the MSP assumes the contractor does. In the assessment, nobody can produce evidence, and the control fails

"We're in GCC High so we're covered."

Microsoft provides the platform controls; you're responsible for the tenant configuration, the identity setup, the DLP rules, and the operational use. Being in GCC High is a start, not an end

"Their SOC 2 covers it."

A provider's SOC 2 audit doesn't automatically satisfy your CMMC requirements. You need a Customer Responsibility Matrix that maps their controls to yours — with your configuration evidence

What a Good CRM Looks Like



Provider-Sourced Foundation

- Start with the provider's published CRM (Microsoft, AWS, and major MSPs all publish one)
- Confirms which controls the provider inherits, shares, or leaves to the customer
- Update to your actual environment — the published version is a template



Per-Control Ownership Assignment

- Every control (all 110) marked: Provider, Customer, Shared, or N/A
- For "Shared": specific configuration or operational split documented
- For "Provider": your obligation is to verify their attestation is current



Evidence Path per Control

- For your controls: pointer to your own evidence artifact
- For provider controls: pointer to the provider's attestation (SOC 2, FedRAMP ATO, ISO 27001)
- For shared controls: both — provider attestation AND your configuration evidence



Living Document, Not One-Time

- Re-verify at each provider contract renewal
- Re-verify when the provider changes their control set
- Re-verify annually as part of SSP review — providers update their CRMs regularly

MSPs and MSSPs: What's Different from Cloud

KEY IDEA

Managed service providers add a wrinkle: they perform controls on your behalf, but they may not be CMMC-assessed themselves. Your documentation has to bridge that gap.

1

The MSP is not your CMMC assessor's problem — they're yours

You are the contractor. The MSP works for you. Your SSP describes what the MSP does; your CRM formalizes the split; your evidence proves both sides are actually happening

2

MSPs handling CUI are External Service Providers (ESPs) under CMMC

ESPs that store, process, or transmit CUI have specific documentation requirements — a contract, a scope statement, and evidence of their security posture. This is not optional

3

Get their SOC 2 Type II — and read it

Not the executive summary. The actual control descriptions and any exceptions. Their control gaps become your control gaps unless you have compensating controls

4

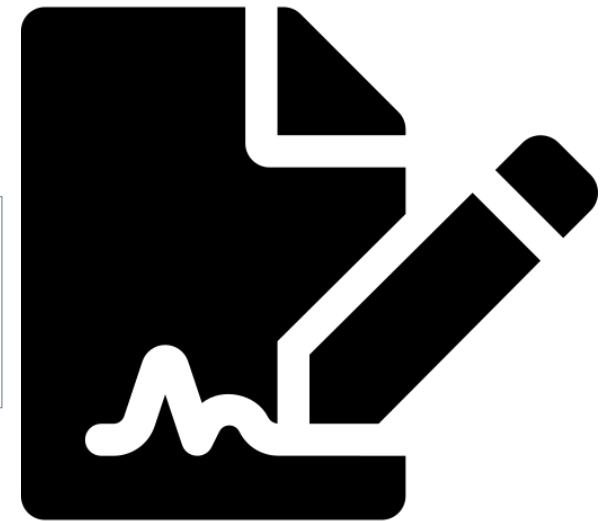
Document what evidence THEY will provide during your assessment

The C3PAO may ask for logs, tickets, or configuration proof from your MSP. If you haven't pre-arranged access or delivery, you'll be scrambling on assessment day

SECTION 5 • THE SYSTEM SECURITY PLAN

The System Security Plan

The master document that pulls the entire package into one story.



What the SSP Is — and What It Isn't

The SSP IS...

A description: Of your CUI environment, its boundary, its components, and how each of the 110 controls is implemented in your specific context

The assessor's map: The document the C3PAO reads first and returns to constantly during the assessment — it structures every conversation

A living document: Version-controlled, dated, reviewed at least annually, updated when the environment or controls change

Executive-signed: Signed by a leadership authority — this represents an organizational commitment, not just an IT deliverable

Traceable: Every control section points to policies, procedures, and evidence that back up the implementation statement

The SSP is NOT...

A policy document: Policies live separately. The SSP references them but does not restate them

A checklist: "Implemented / Not Implemented / Partially" is not enough. The SSP explains HOW each control works in your environment

A generic template: Templates give you structure. But an SSP that reads like the template is an SSP that describes nobody's real environment

Aspirational: It describes what you do today — not what you plan to do. Gaps go in the POA&M, not in the SSP

An IT-only document: It reflects the whole organization's cybersecurity posture — governance, HR, physical security, third parties

Anatomy of a Strong SSP



System Identification & Boundary

- System name, purpose, categorization, and operational status
- Boundary definition — what's in scope for CUI
- Data flows showing how CUI enters, is stored, and leaves the boundary
- Network diagram showing systems, subnets, and connections



Per-Control Implementation

- Statement for each of the 110 controls (or 320 objectives if more granular)
- Describes HOW the control operates in your environment
- References supporting policies, procedures, and evidence
- Marked METs, gaps flow to the POA&M



Assets & Roles

- Asset inventory — hardware, software, firmware, virtual, cloud tenants
- External Service Providers with their scope of involvement
- Roles and responsibilities — who owns what
- Key personnel: system owner, ISSO/ISSM, CISO



Governance & Maintenance

- Approval page — executive signature and date
- Revision history with change descriptions
- Review cadence — annually at minimum
- Distribution and access controls (the SSP is itself CUI in most cases)

Writing Implementation Statements Assessors Accept

KEY IDEA

Every implementation statement should answer four questions: what does the control do, how does it operate in our environment, who is responsible, and where is the evidence. Statements missing any of the four are the #1 cause of assessor callbacks.

1**WHAT: State the control outcome in your own words**

Not a paraphrase of the control text — a plain-English description of what the control accomplishes here. "All privileged access to CUI systems requires multi-factor authentication"

2**HOW: Name the specific mechanism**

Tool, technology, or process by name. "Enforced through Microsoft Entra ID Conditional Access policy 'CUI-Admin-MFA-Required' with phishing-resistant methods (FIDO2 or Windows Hello for Business)"

3**WHO: Name the role responsible**

"The Identity and Access Management team owns policy configuration; the Security Operations Center monitors for policy bypass attempts"

4**WHERE: Point to supporting documentation**

"See Access Control Policy §3.2, MFA Enrollment Procedure, and evidence library folder /AC-2/ for the current policy configuration export and enrollment reports"

The Single Most Common SSP Failure: Boundary Definition

WHY IT MATTERS

The boundary defines what's in scope. If it's fuzzy, ambiguous, or drawn too broadly, the assessment gets harder, longer, and more expensive. If it's drawn too narrowly and CUI leaks outside it, you fail. A well-defined, defensible boundary is the single highest-leverage decision in the SSP.

Draw the boundary around CUI — not around convenience

The boundary contains everything that stores, processes, or transmits CUI. It does not contain your corporate wiki or your marketing website just because they're on the same network

Enclaved or all-hands: choose deliberately

Enclaved (isolated CUI environment) shrinks the boundary and the assessment scope. All-hands (whole corporate network in scope) is simpler but massively more expensive. This is a business decision, not a technical one

Document connections through the boundary

Every path CUI takes in or out — email, file transfer, VPN, cloud sync — needs to be identified, justified, and controlled. Undocumented paths become findings

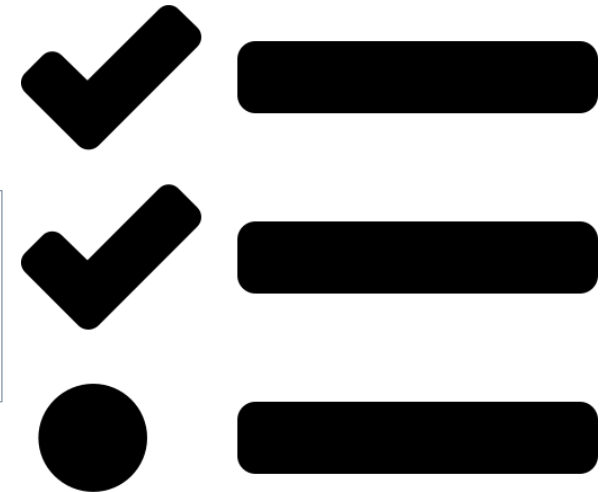
Update the boundary when the environment changes

New system? Boundary review. New cloud service? Boundary review. Merger, acquisition, remote workforce change? Boundary review. Static boundaries in dynamic environments are stale by day 30

SECTION 6 • THE POA&M

The Plan of Action and Milestones

How you track and remediate what isn't yet fully in place — with discipline.



What the POA&M Is — and Isn't

THE BIG IDEA

The POA&M is a formal, dated, ownership-assigned register of every unmet or partially-met requirement, with a documented plan to close each gap. Under CMMC L2, only a limited set of controls can be POA&M'd, and each item has a required closure deadline.

1

IT IS

A Formal Register

Structured document listing every unmet or partially-met requirement, the plan to fix it, the owner, the target completion date, and the current status. Updated on a defined cadence, reviewed at leadership level.

2

IT IS NOT

A Wish List or To-Do List

A POA&M is not the place for "things we'd like to do someday." Items must have concrete plans, real owners, and realistic dates. Anything vague, unassigned, or open-ended is a POA&M failure.

3

IT IS NOT

A Hiding Place

Some organizations POA&M controls they could just implement. Under CMMC L2, this doesn't work — POA&M-eligible controls are limited, and items must close within 180 days. You can't hide indefinitely.

BOTTOM LINE A clean POA&M with legitimate items and demonstrable progress is a sign of a mature program. A stale POA&M with items open for years is a red flag — often more damaging than the gaps themselves.

Building a Defensible POA&M

Required Fields (Every Item)

- Control ID and assessment objective(s) not met
- Description of the gap in specific, factual terms
- Planned remediation approach
- Owner (named role, not person)
- Target completion date, status, and last-updated date

Under CMMC L2: Timing Matters

- POA&M items must close within 180 days of assessment
- Only certain controls are POA&M-eligible (defined in the CMMC rule)
- Some controls ("showstoppers") cannot be POA&M'd at all
- Miss the 180-day window and you lose your certification

Cadence and Governance

- Reviewed at least monthly by security leadership
- Reviewed quarterly by executive leadership
- Every review meeting produces minutes — those are evidence
- Reviewed at every SSP revision

Common Failure Modes

- Items open for a year with no visible progress
- Dates that keep slipping without explanation
- "TBD" owners or "ongoing" completion dates
- Items that describe symptoms, not root causes

POA&M Discipline: What Separates Mature Programs From Failing Ones

KEY IDEA

The POA&M is the document that most obviously reveals whether an organization actually runs its cybersecurity program or just documents that it exists. Assessors read the POA&M like a diary.

1**Every item has visible movement**

Between review cycles, something should have changed — a milestone completed, a status update, a revised plan. Items frozen in place suggest nobody actually owns them

2**Items close and get archived**

When a POA&M item is done, it doesn't disappear — it moves to a closed section with the completion date and the evidence of closure. This shows the process works

3**New items get added deliberately**

When a new gap is identified — from a scan, an audit, a security review — it gets added to the POA&M within a short window. Gaps discovered but not tracked are gaps ignored

4**Dates are realistic, not optimistic**

A POA&M full of past-due items is worse than a POA&M with realistic future dates. Set dates you can actually meet, and update them honestly when they slip

5**Ownership is at a role level, and roles are staffed**

"Owner: IT Director" only works if there's an IT Director. Vacant roles owning open items is a red flag — the gap has no actual owner

SECTION 7 • PUTTING IT TOGETHER

Putting It Together

How the package works as one coherent story on assessment day.

The Documentation Package as One Coherent Story

THE BIG IDEA

By assessment day, everything you've built has to work as a single integrated package. The assessor should be able to walk from the SSP to a policy, from a policy to a procedure, from a procedure to evidence — without gaps, contradictions, or dead ends.

1**STARTS HERE**

The SSP Points the Way

The assessor opens the SSP and reads the implementation statement for a control. That statement references specific policies, procedures, and evidence. The assessor follows those references — they must resolve.

2**MOVES THROUGH**

Policies & Procedures Explain

The referenced policy shows authority and scope. The referenced procedure shows the operational detail. Both are current, approved, and describe the environment as it actually is.

3**LANDS AT**

Evidence Proves It

The referenced evidence artifact confirms the procedure actually ran. It's dated, current, and satisfies the assessment objective. The chain closes.

BOTTOM LINE When this chain works for every control, you pass. When it breaks anywhere — missing evidence, stale policy, procedure not describing reality — that specific control fails. Coherence across the package is what an assessment measures.

The Start-Monday List: Your First Week Building Documentation

KEY IDEA

If you're starting from zero — or from a pile of unstructured template artifacts — here's the sequence that gets you the most defensible position the fastest.

1**Draw your boundary diagram**

A simple, defensible visual of what's in scope for CUI — systems, users, connections, external providers. Everything else builds on this. Get it in front of leadership for review

2**Inventory your existing documentation**

What policies, procedures, and evidence do you already have? Even if they're not CMMC-aligned. The gap between what you have and what you need is your work list

3**Choose your policy structure and build a template**

One-per-family or master document — pick one and commit. Build the template with required elements (approval, scope, roles). This alone unblocks a lot of downstream work

4**Start the evidence library structure**

Empty folders per control (or per objective). Naming convention documented. Access controls in place. When evidence starts flowing, it goes into the right place from day one

5**Start the SSP shell around the boundary**

Sections 1 and 2 (system identification, assets, roles) can be written now. Per-control statements come later, but the structure and the boundary description do not need to wait

6**Open the POA&M on day one**

Every gap you identify goes in immediately, with an owner and a target date. This is not a document that gets built after the assessment — it's a document that lives throughout the program



An APEX Accelerator

Questions?

Let's talk about your specific documentation gaps.



WISCONSIN PROCUREMENT INSTITUTE

Matthew Frost · Government Contract Specialist

mattf@wispro.org

No cost help for Wisconsin businesses

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 16 – 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

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