Acquisition Hour:

An Introduction into the Supplier Performance Risk System (SPRS)

March 11 | Noon – 1:00 pm

Presented by:
Matt Frost, Wisconsin Procurement Institute

Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

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.

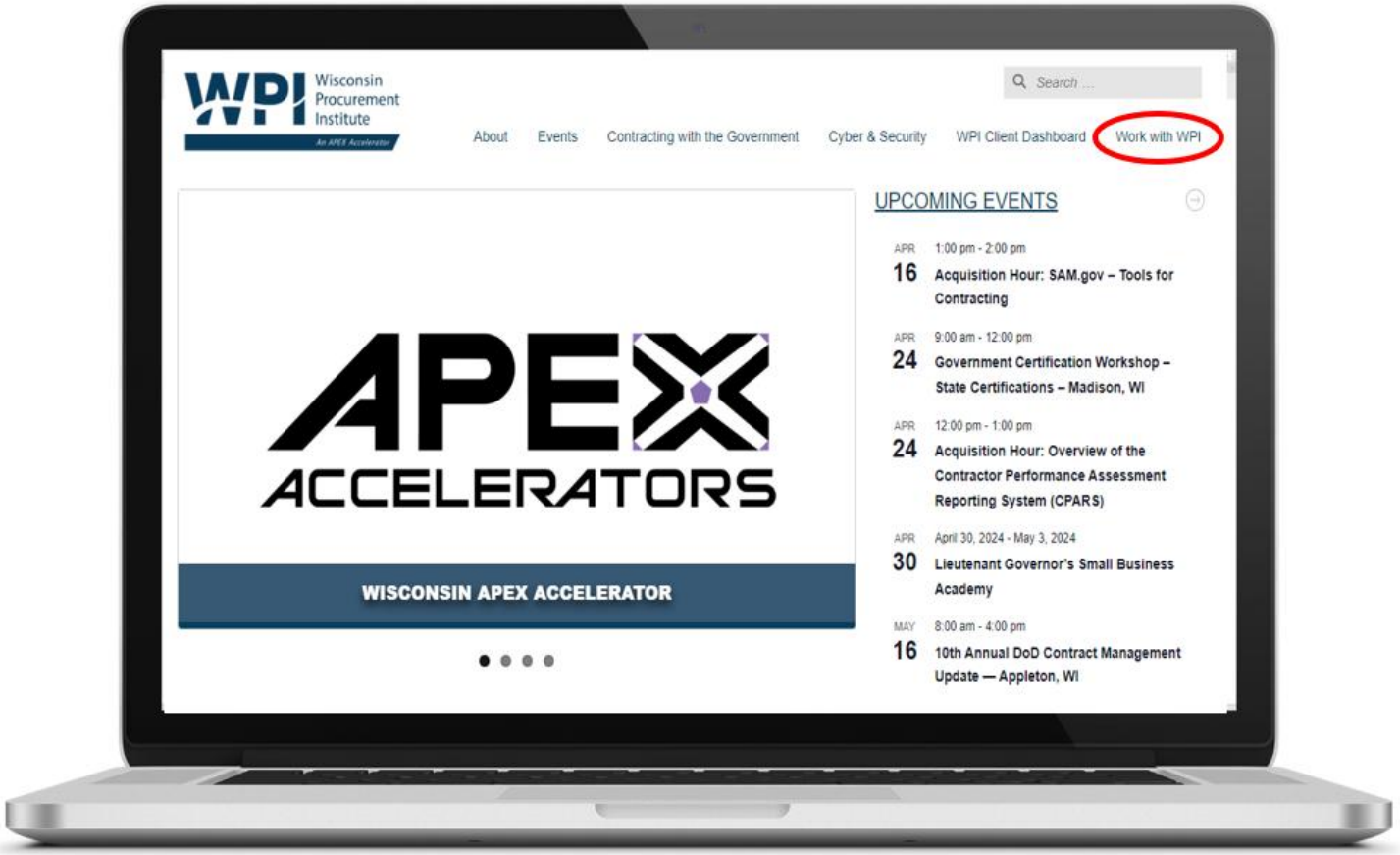
WPI provides services and training to all of Wisconsin's 72 counties

- 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

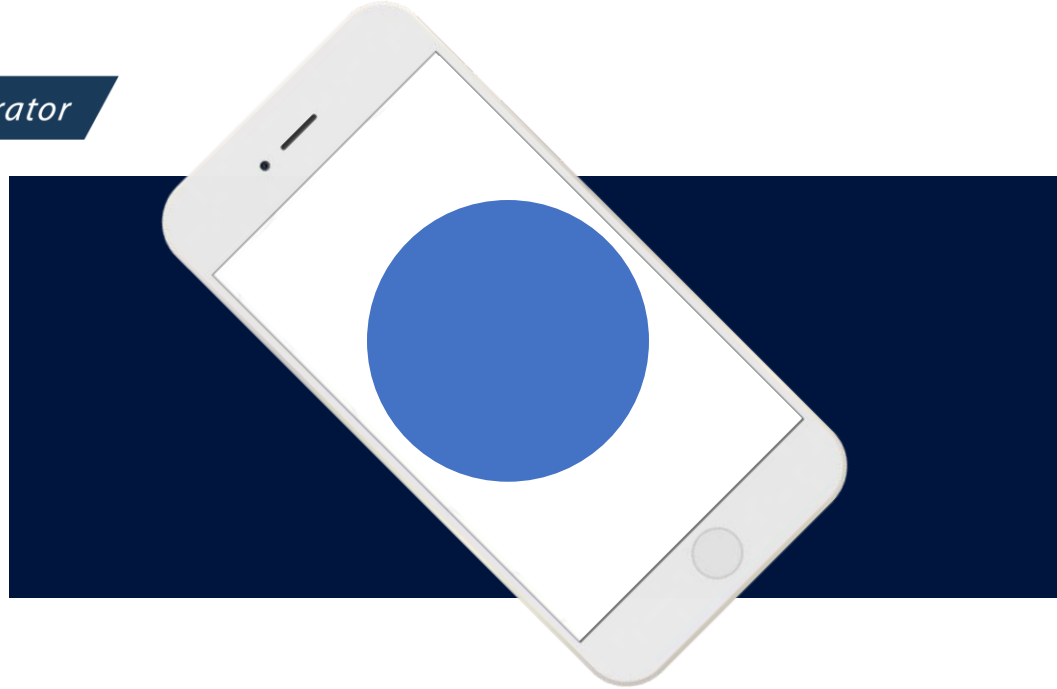
- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND 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

Wisconsin Procurement Institute

An APEX Accelerator

Supplier Performance Risk System (SPRS)



Acquisition Hour – March 11th, 2026

SUPPLIER PERFORMANCE

RISK SYSTEM

S P R S

A Comprehensive Introduction for DoD Suppliers & Industry Partners

Covering: Supplier Performance · Price/Cost Data · Cybersecurity · CMMC

TODAY'S AGENDA

What We'll Cover

01 **SPRS: The Full Picture**

All the ways DoD uses SPRS beyond cybersecurity

02 **Supplier Performance Data**

Past performance, quality, delivery & awards

03 **Price & Cost Data**

How SPRS informs price reasonableness determinations

04 **Origins & History**

Legislative background & DFARS 252.204-7012

05 **Cybersecurity Scoring**

NIST SP 800-171 self-assessment methodology

06 **Why It Matters**

Contract eligibility & risk implications

07 **CMMC & the Road Ahead**

How SPRS fits into the evolving compliance landscape

08 **Action Items**

Steps suppliers must take right now

SECTION 01

SPRS: The Full Picture

More than cybersecurity — a DoD-wide enterprise risk tool

What Is SPRS?

SPRS (Supplier Performance Risk System) is a DoD enterprise web application maintained by the **Defense Logistics Agency (DLA)**. It is the primary system DoD uses to assess, store, and share risk data about contractors — covering performance, pricing, and cybersecurity.

Supplier Performance

Tracks past performance ratings, quality deficiencies, delivery metrics, and awards/deductions across DoD contracts.

Price & Cost Data

Stores historical price and cost information used by Contracting Officers to assess price reasonableness and negotiate fair contracts.

Cybersecurity Risk

Holds NIST SP 800-171 self-assessment scores that measure a supplier's ability to protect Controlled Unclassified Information (CUI).

Pre-Award Research

All DoD Contracting Officers are required to check SPRS before awarding contracts — it's the single authoritative risk lookup tool.

DoD-Wide Visibility

Used by Army, Navy, Air Force, SOCOM, DLA, DCSA, and every other DoD Component. One score; visible to all.

Industry-Facing

Any company seeking DoD work must understand SPRS. It affects award eligibility, pricing negotiations, and compliance standing.

The Three Pillars of SPRS

01 Supplier Performance

- Past performance ratings (CPARS/PPIRS)
- Quality deficiency reports (QDRs)
- Delivery performance metrics
- Award/deduction history
- Contractor-held inventory data

02 Price & Cost Data

- Historical unit price data by NSN/contract
- Price trends across multiple awards
- Comparison against market benchmarks
- Used for price reasonableness analysis
- Informs sole source and competitive awards

03 Cybersecurity Risk

- NIST SP 800-171 self-assessment score
- Score range: −110 to +110
- Date of last assessment on file
- Required for contracts involving CUI
- Foundation for CMMC compliance pathway

SECTION 02

Supplier Performance Data

How DoD tracks and uses contractor performance history

What Supplier Performance Data Lives in SPRS

Data Sources Fed Into SPRS

CPARS

Contractor Performance Assessment Reporting System — government evaluations of contractor quality, schedule, cost, and management on contracts ≥$1.5M (services) or $750K (construction).

PPIRS

Past Performance Information Retrieval System — legacy system now integrated into CPARS providing historical performance ratings dating back decades.

FAPIIS

Federal Awardee Performance & Integrity Info System — records terminations for cause, defective pricing determinations, and administrative agreements.

QDRs

Quality Deficiency Reports — formal records of delivered items that fail specifications. Tracked by NSN and contractor.

How Contracting Officers Use This Data

Pre-Award Evaluation

COs must assess past performance as a source selection factor. SPRS is the primary lookup. Poor ratings can make a vendor technically unacceptable.

Price Negotiation

Performance history informs whether a vendor's pricing premium is justified — or whether it's a risk requiring reduction.

Delivery Risk Assessment

Recurring late deliveries flagged in SPRS can trigger additional scrutiny, performance bonds, or liquidated damages clauses.

Responsibility Determination

Consistent poor performance can support a finding that a contractor is 'non-responsible' — blocking award entirely.

CPARS Performance Ratings: What They Mean for You

CPARS ratings are entered by government evaluators and visible to any Contracting Officer nationwide. They follow a contractor for years.

Exceptional ~5% of ratings	Performance significantly exceeds requirements. Reserved for truly outstanding execution. Highly competitive advantage in source selection.
Very Good ~25% of ratings	Performance exceeds requirements. Positive indicator in past performance evaluations. Strong competitive position.
Satisfactory ~55% of ratings	Performance meets requirements. Neutral competitive factor. Most contractors fall here. Not a differentiator.
Marginal ~10% of ratings	Performance does not meet some requirements. Requires corrective action. Can be overcome with evidence of improvement.
Unsatisfactory ~5% of ratings	Fails to meet requirements. Serious red flag. Can support a non-responsibility determination. Extremely damaging to award eligibility.

SECTION 03

Price & Cost Data

How SPRS supports price reasonableness and negotiations

How SPRS Stores & Uses Price and Cost Data

SPRS maintains a repository of historical contract pricing that Contracting Officers use to validate whether proposed prices are fair and reasonable.

$Trillions
in historical contract data

NSN-Level
pricing by national stock no.

Multi-Year
price trend analysis

Real-Time
accessible to all DoD COs

What's Stored

- Unit prices paid per contract line item (CLIN)
- Quantities purchased and delivery dates
- Contract type (FFP, T&M, CPFF, etc.)
- Contractor identity and CAGE code
- NSN / item description linkage

How COs Use It

- Compare proposed price to prior awards for same item
- Identify price spikes that warrant closer scrutiny
- Support price analysis in lieu of cost analysis
- Negotiate better pricing using historical benchmarks
- Document price reasonableness determinations

What This Means for Suppliers: Pricing Transparency

Because Contracting Officers can see your pricing history, suppliers must understand how past prices affect future negotiations.

Price Increase Scrutiny

If you propose a higher unit price than your last award for the same item, expect the CO to question it. You'll need documented cost justification — material cost increases, labor rate changes, or design modifications.

Competitive Advantage Visibility

Suppliers who consistently offer competitive pricing build a verifiable track record in SPRS. This can be a differentiator when a CO is assessing risk between vendors.

Sole Source Negotiations

In sole source awards, COs rely heavily on SPRS price history when there's no competition to establish fair market value. Your previous prices become the baseline for negotiation.

Price Reasonableness Challenges

If your proposed price is significantly higher than SPRS history — without clear justification — the CO may determine price reasonableness cannot be established, blocking or delaying award.

SECTION 04

Origins & History

The regulatory journey from 2016 to today

SPRS Before DFARS 252.204-7012: The 30-Year Foundation

SPRS did not emerge from the cybersecurity mandate — it evolved over three decades as a Navy-born supply chain quality and risk tool before DoD adopted it enterprise-wide.

1989 → 2006–2007 → 2018

PDREP

Product Data Reporting & Evaluation Program

Managed by: Naval Sea Logistics Center Portsmouth (Navy)

- Created to collect quality deficiency & delivery data across the Department of the Navy supply chain
- Tracked Product Quality Deficiency Reports (PQDRs), Supply Discrepancy Reports (SDRs), and contract delivery performance
- Built as a DON-specific tool — not yet DoD-wide — to hold suppliers accountable for quality and on-time delivery
- Established the foundational data architecture that would underpin all future systems
- Still operates today as the authoritative DON repository feeding SPRS

PPIRS-SR NG

Past Performance Info Retrieval System – Statistical Reporting Next Gen

Managed by: DoD-wide expansion of PDREP concept

- PDREP introduced its Red / Yellow / Green (R/Y/G) contractor risk scoring algorithm in 2007
- Vendor Performance: quality & delivery scores by Federal Supply Class (FSC), Product Service Code (PSC), and NAICS
- Supplier Risk scoring expanded to rank 79,000+ CAGE codes across DoD — not just the Navy
- Price Risk module added: compared proposed prices against historical government purchase data for 1.6M+ items
- Item Risk module flagged suspected counterfeit parts, diminishing manufacturing sources (DMSMS), and other item-level risks

SPRS

Supplier Performance Risk System (formal rename & expansion)

Managed by: DLA / DoD enterprise — all components

- PPIRS-SR NG officially renamed SPRS in Q1 FY2018 with major enhancements and a database upgrade
- Scope expanded to all DoD Components: Army, Navy, Air Force, SOCOM, DCSA, DLA and beyond
- DoDI 5000.79 (2019) codified SPRS as the authoritative DoD-wide source for Supplier & Product Performance Information
- Cybersecurity assessments (NIST SP 800-171) added as a new data layer — DFARS 252.204-7012 context created the demand
- The same 30-year performance/pricing foundation now carries the cybersecurity scores contractors know today

Legislative & Regulatory Timeline

2016

DFARS 252.204-7012 Issued

DoD interim rule requiring contractors handling CUI to implement NIST SP 800-171 and report cyber incidents within 72 hours.

2019

SPRS Cybersecurity Scores Introduced

DoD begins requiring self-assessment score submissions. Scores must reflect NIST SP 800-171 implementation status.

2020

DFARS Class Deviation 2019-O0003

Formal mandate: SPRS score submission required before any new contract award involving covered defense information.

2021

DFARS 252.204-7019 / 7020 Final

Interim rules finalized: minimum score of −170 required (or POA&M). Medium/high assessments introduced for sensitive programs.

2024+

CMMC 2.0 Phase-In Begins

Third-party CMMC certifications begin phasing into contracts. SPRS scores serve as the interim mechanism during transition.

SECTION 05

Cybersecurity Scoring

NIST SP 800-171 DoD Assessment Methodology

DFARS 252.204-7012: The Foundation

Core Requirements

- Implement all 110 controls in NIST SP 800-171
- Report cyber incidents to DoD within 72 hours
- Provide DoD access to systems for damage assessment
- Flow down requirements to subcontractors handling CUI
- Maintain a System Security Plan (SSP)
- Track gaps in a Plan of Action & Milestones (POA&M)

Who Is Covered?

- Prime contractors on DoD contracts involving CUI
- Subcontractors who process, store, or transmit CUI
- Cloud service providers handling CUI
- Companies bidding on covered contracts

⚠ Key Point

DFARS 252.204-7012 applies whenever a contract involves Covered Defense Information (CDI) — which broadly includes any Controlled Unclassified Information (CUI). If your contract touches sensitive DoD data, you are almost certainly covered.

The NIST SP 800-171 Self-Assessment Score

110

Controls

How Your Score Is Calculated

1. **Start at 110 points**

   Maximum score = 110. One point per fully implemented control.

2. **Deduct for gaps**

   Controls NOT fully implemented deduct 1–5 pts each by criticality. Max deduction −203 pts (floor = −110).

3. **Document your SSP**

   Your System Security Plan must describe how each control is—or will be—implemented.

4. **Log in SPRS**

   The responsible official inputs the score at sprs.apps.mil. Assessment date is recorded.

5. **Update regularly**

   Scores must reflect current posture. Update after significant changes or remediation.

Understanding Score Ranges

110 Perfect Score	All 110 controls fully implemented. Highest achievable score. Demonstrates fully mature cybersecurity posture.
88–109 Strong Posture	Most controls implemented; minor gaps in POA&M. Competitive for award. Most CMMC-prepared companies land here.
1–87 Partial Compliance	Meaningful gaps remain. POA&M required. Award possible depending on program sensitivity and CO risk tolerance.
-110 – 0 Significant Risk	Substantial non-compliance. Many agencies will still award with strong POA&M showing near-term remediation milestones.
Below -110 Severe Risk	Critical controls unimplemented. Very unlikely to receive award. Immediate remediation plan mandatory.

SECTION 06

Why It Matters

Contract eligibility, risk, and real-world consequences

Impact on Contract Awards

Under DFARS 252.204-7019 and 7020, a current SPRS score is a condition of contract award for contracts involving CUI.

⚠ If No Valid Score

- CO may not award the contract
- May be found technically unacceptable
- Existing contracts may face scrutiny at option exercise
- Cannot demonstrate minimum cybersecurity posture
- Competitive disadvantage vs. compliant peers

✓ With a Valid Score

- Eligible for contract award consideration
- Demonstrates proactive compliance to CO
- Foundation for CMMC certification
- Builds trust with primes and government
- Positions company for expanded DoD work

The Risk of Inaccurate Scores

False Claims Act (31 U.S.C. §§ 3729–3733) Exposure

Knowingly submitting an inflated or inaccurate SPRS score may constitute a false claim to the government, carrying treble damages and civil penalties.

Financial Penalties

Treble (3×) damages on contract value plus civil penalties of $13,000–$27,000 per false claim submitted.

DOJ Prosecution

The Dept. of Justice has actively pursued contractors for cybersecurity misrepresentation under the DoD's Civil Cyber-Fraud Initiative since 2021.

Suspension & Debarment

False statements can trigger debarment proceedings, barring a company from future federal contracting government-wide.

Reputational Damage

DOJ investigation disclosures cause lasting reputational harm in the defense industrial base and with prime contractors.

SECTION 07

CMMC & the Road Ahead

Where SPRS fits in the evolving compliance landscape

CMMC 2.0 & SPRS: Complementary Frameworks

L1 — Foundational	L2 — Advanced	L3 — Expert
Controls	**Controls**	**Controls**
17 FAR 52.204-21 practices	110 NIST SP 800-171 practices	110+ practices including NIST SP 800-172
Assessment Method	**Assessment Method**	**Assessment Method**
Annual self-attestation by senior company official	Triennial 3rd-party assessment (C3PAO) for priority programs; self-assessment for others	Triennial government-led assessment by DCSA DIBCAC
SPRS Role	**SPRS Role**	**SPRS Role**
No SPRS score required for L1	SPRS score required as interim measure until C3PAO assessment	SPRS score + DIBCAC high-level assessment required

SECTION 08

Action Items

Steps your organization must take now

Supplier Action Checklist: All Three SPRS Pillars

01 Supplier Performance

IMMEDIATE

Register in PIEE / SPRS

Obtain PIEE access (piee.eb.mil) to view your company's SPRS data, scores, and CAGE hierarchy. A CAC or PKI certificate is required.

IMMEDIATE

Review Your CPARS Ratings

Log into CPARS (cpars.gov) and review every active and recent past performance evaluation. You have 14 days to comment on draft ratings — use that window.

NEAR-TERM

Respond to Negative Evaluations

Contest factually incorrect CPARS entries through the official dispute process. Document strong performance with data — on-time delivery rates, quality metrics, customer feedback.

ONGOING

Monitor QDR / SDR Records

Track Quality Deficiency Reports and Supply Discrepancy Reports in PDREP. Patterns of QDRs are visible to COs and will suppress your Supplier Risk score.

ONGOING

Build a Performance Track Record

02 Price & Cost Data

IMMEDIATE

Understand Your Price History

COs can see every price you've been paid for every item by NSN. Know your own history before you submit a proposal so you're not caught off guard.

IMMEDIATE

Document Cost Drivers

If your costs have increased since your last award, build the documentation now: supplier invoices, labor rate agreements, material cost data. Have it ready before negotiations begin.

NEAR-TERM

Align Proposals to Market

Use SPRS price history (visible through your PIEE account) to gauge how your pricing compares. Outliers — high or low — will draw scrutiny.

NEAR-TERM

Prepare for Sole Source Scrutiny

On sole source awards, your prior SPRS prices ARE the benchmark. Prepare a written price justification narrative for any increases, referencing material or labor cost changes.

ONGOING

Maintain Clean Delivery Records

03 Cybersecurity

IMMEDIATE

Submit a Current SPRS Score

A valid NIST SP 800-171 self-assessment score is required for contract award on CUI-covered work. Log in to sprs.apps.mil and submit. An absent or expired score blocks award.

IMMEDIATE

Conduct a Gap Assessment

Compare your security environment against all 110 NIST SP 800-171 controls. Identify what's implemented, what's partial, and what's missing before scoring.

NEAR-TERM

Build / Update Your SSP

Your System Security Plan must describe how each of the 110 controls is implemented (or will be). It is a contractual deliverable — not optional — and the foundation of your compliance posture.

NEAR-TERM

Create a POA&M

Document every unimplemented control with realistic remediation milestones. A credible POA&M demonstrates commitment and can offset a lower score during CO review.

ONGOING

Plan for CMMC Certification

Supplier Action Checklist

01 IMMEDIATE

Register in SPRS

Ensure your company is registered. Access requires a CAC or PKI certificate via sprs.apps.mil.

02 IMMEDIATE

Conduct a Gap Assessment

Compare current security controls against NIST SP 800-171 Rev 2. Identify which of 110 controls are implemented.

03 NEAR-TERM

Build Your SSP

Document how each control is implemented (or will be). Required by contract and demonstrates due diligence.

04 NEAR-TERM

Create a POA&M

For unimplemented controls, document a realistic plan with milestones. Shows commitment to compliance.

05 NEAR-TERM

Calculate & Submit Score

Use the DoD NIST SP 800-171 Assessment Methodology to calculate your score and submit to SPRS.

06 ONGOING

Plan for CMMC

Determine your required CMMC level. Begin preparing for third-party assessment if Level 2 is needed.

Key Resources & References

SPRS Portal
sprs.apps.mil

Official DoD portal for submitting and viewing SPRS scores. Requires PKI certificate or CAC.

NIST SP 800-171 Rev 2
nvlpubs.nist.gov

The 110 cybersecurity requirements. Definitive reference. Free download from NIST.

DoD Assessment Methodology
dodcio.defense.gov

Official scoring guide for calculating your NIST SP 800-171 self-assessment score.

CMMC Accreditation Body
Cyberab.org

Marketplace for C3PAOs and Registered Practitioners. CMMC L2 assessment resources.

DFARS Clauses (7012/7019)
acquisition.gov

Full text of the DoD cybersecurity and SPRS contract clauses on the FAR/DFARS site.

CPARS System
cpars.gov

Contractor Performance Assessment Reporting System — view and respond to past performance evaluations.

Questions & Discussion

KEY TAKEAWAYS

- SPRS is the DoD's all-in-one risk system — performance, pricing, and cybersecurity
- Your SPRS data directly affects award eligibility, price negotiations, and compliance standing
- Inaccurate scores carry serious False Claims Act liability — score honestly
- CMMC is coming — SPRS is your bridge; start building your compliance posture now

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.

- **March 11** – An Introduction into the Supplier Performance Risk System (SPRS)
- **March 18** – Department of Defense Invoicing – PIEE / Wide Area Workflow

…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.

- ~~**February 26** – CMMC: Control Set Series: 3.1 Access Control~~
- **March 26** – CMMC: Control Set Series: 3.2 Awareness and Training
- **April 30** – CMMC: Control Set Series: 3.3 Audit and Accountability
- **May 28** – CMMC: Control Set Series: 3.4 Configuration Management

…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.

- **March 17** – Government Property Programs
- **March 24** – OTAs and Consortiums
- **March 31** – CRADAs: Cooperative Research and Development Agreements
- **April 7** – Does Your Business Specialize in Critical Technology Areas?
- **April 14** – Unlocking DoD Opportunities for Nontraditional Contractors

…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 Innovation Drive Suite 320
Milwaukee WI 53226
414-270-3600