Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

Cyber Friday

Managing Vendor Risk

March 19, 2021




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 34 Years of serving Wisconsin Business!

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, State and Local Government contracts.

- **INDIVIDUAL COUNSELING – At our offices, at client's facility or via telephone/GoToMeeting**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

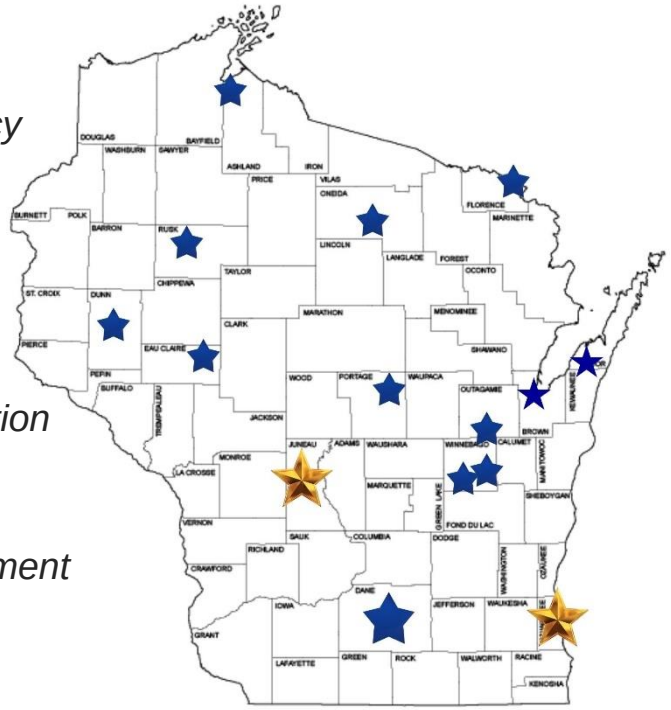
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

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)*
- **STEVENS POINT**
  - *IDEA Center*
- **APPLETON**
  - *Fox Valley Technical College*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*
- **OSHKOSH**
  - *Fox Valley Technical College*
  - *Greater Oshkosh Economic Development Corporation*
- **EAU CLAIRE**
  - *Western Dairyland*
- **MENOMONIE**
  - *Dunn County Economic Development Corporation*
- **LADYSMITH**
  - *Indianhead Community Action Agency*
- **RHINELANDER**
  - *Nicolet Area Technical College*
- **ASHLAND**
  - *Ashland Area Development Corporation*
- **FLORENCE**
  - *Florence County Economic Development*
- **DOOR COUNTY**
  - *NE WI Technical College*
  - *Door County Economic Development Corporation*



3/19/21

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Cyber Friday

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

Managing Vendor Risk

Marc N. Violante

March 19, 2021

Current requirements

- Federal –
  - 52.204-21 -- Basic Safeguarding of Covered Contractor Information Systems (Jun 2016)
- DoD –
  - 252.204-7012 --SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
  - 252.204-7019 -- NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)
  - 252.204-7020 -- **NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS** (NOV 2020)
    - DoD Basic Assessment Methodology
      - CAGE, Date Assessment Performed, SSP name (if more than one), Brief Architecture Description, Summary Score, Date a score of 110 will be achieved – upload to SPRS
      - Flow down – assessment can be performed and emailed to webptsmh@navy.mil for posting to SPRS.
- Other requirements listed in solicitation/contract* -- RFQ's

CMMC moving forward

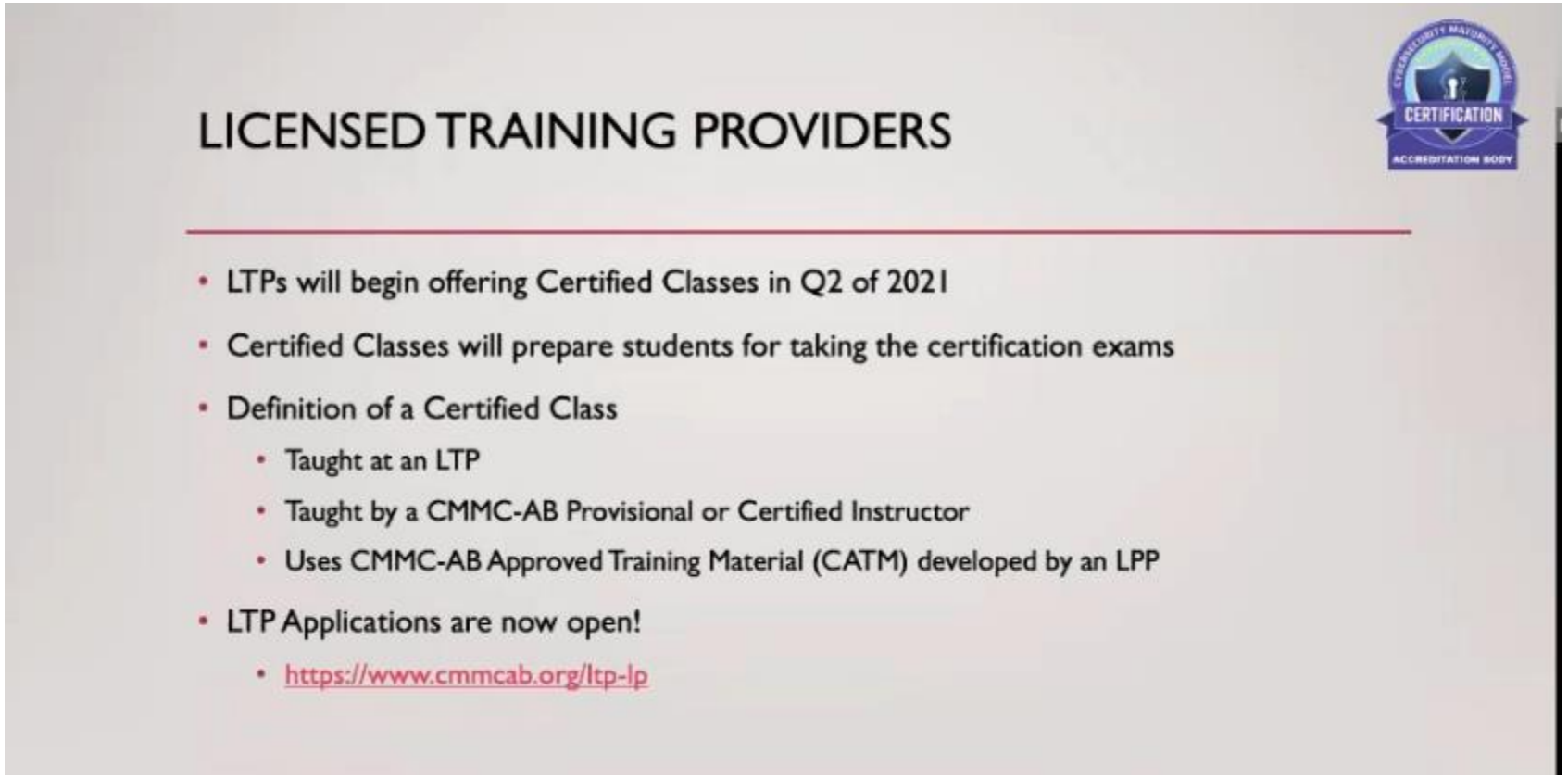
Subsequently changed to USD (A&S) CISO – Ms. Arrington*

- The Department is implementing CMMC through a phased rollout approach - FY2021-FY2025
- Until September 30, 2025, the Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the inclusion of the CMMC requirement in any solicitation.
- These contracts will focus on mid-sized programs that require the contractor to process or store CUI (CMMC Level 3). Primes will be required to flow down the appropriate CMMC requirement to their subcontractors.

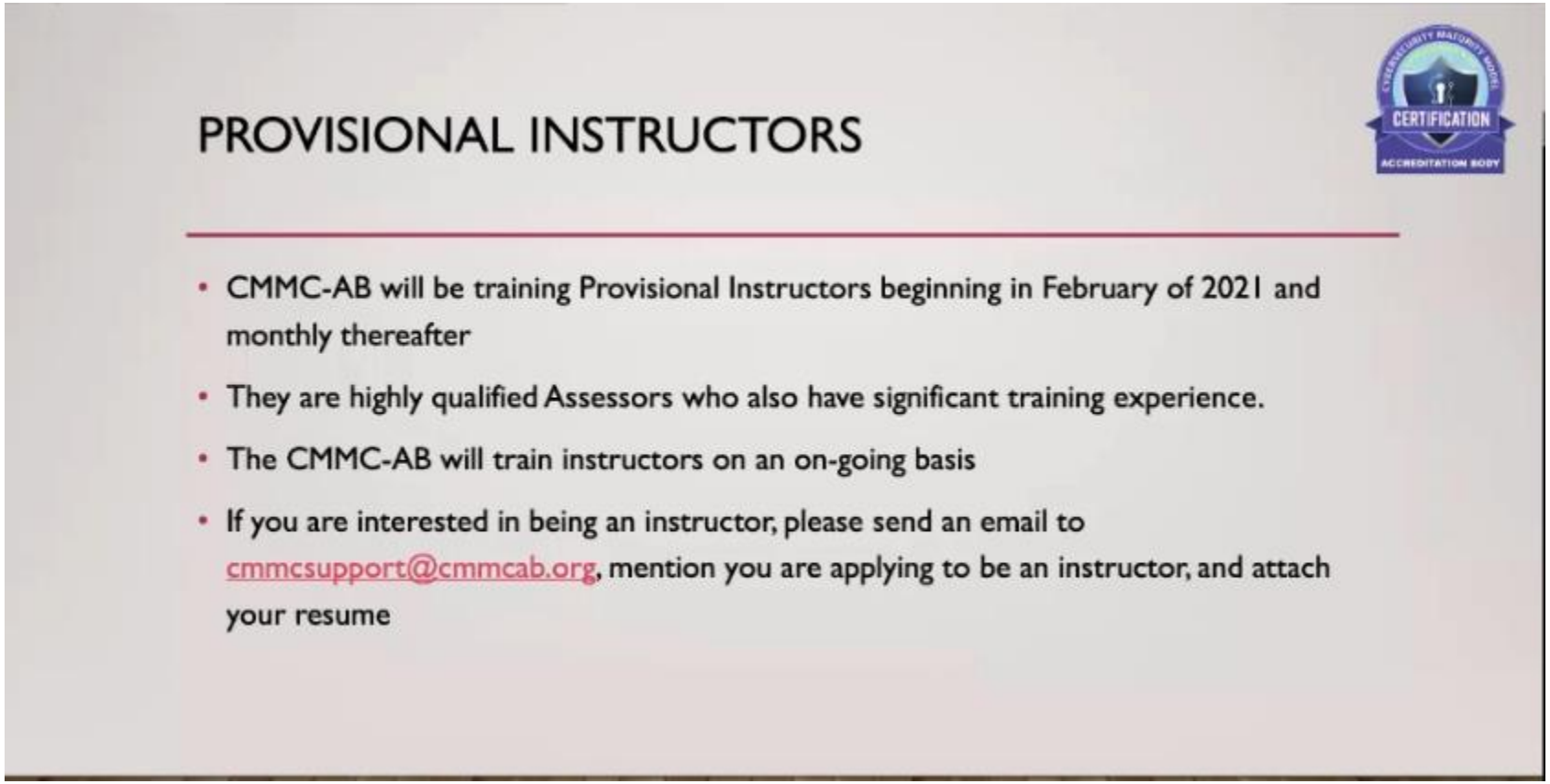
FY2021	FY2022	FY2023	FY2024	FY2025
15	75	250	325	475

https://www.acq.osd.mil/cmmc/faq.html FAQ - 26
*CMMC-AB January Townhall, comments

CMMC-AB: update items (1)



CMMC-AB: update items (2)



Pilot Key Takeaways

Until 1 Oct 2025, CMMC requirements will only be included in new acquisitions with the approval of OUSD(A&S) / OCISO(A&S)

CMMC Pilot programs will include applicable CMMC requirements in RFPs

- OUSD(A&S) is not funding CMMC Pilots
- CMMC certification must be met by contract award
- CMMC certification is required of the enterprise network or particular segment where FCI or CUI is processed, stored, or transmitted in performance of the particular contract
- CMMC certification must be maintained for the duration of the contract; recertification may be necessary depending on expiration date of the CMMC certification versus the contract end date

CMMC Pilot contractors will be required to achieve CMMC Certification

- DIB Contractor enters into Business Relationship with an authorized / approved C3PAO
- CMMC certification is achieved by passing a CMMC assessment conducted by C3PAO
- All CMMC practices and processes must be implemented at the required CMMC Level
- CMMC does not allow POAMs
- If there are assessment findings, the contractor will need to remediate to achieve CMMC certification
- CMMC Certification is good for three years

OUSD(A&S) will provide guidance and support during Pilot roll-outs

10

Develop – processes, procedures (good habits) = **Institutionalization**

Don’t Develop “tunnel vision” re: CMMC

United States Air Force

Weapon System
Program Protection / Systems Security Engineering
Guidebook

Version 2.0

12 March 2020

All the blocks are checked – now what?

- ✓SAM
- ✓JCP
- ✓ITAR
- ✓DoD Basic Assessment

Are they?

Beware of Confirmation Bias

- What is better?
  - To seek “Yes” and overlook what’s missing
  - To find “No’s” correct those discrepancies and develop a system that creates a strong “Yes?

The Role of Culture as a Governance Tool to Achieve Cybersecurity

- Organizational culture is the underlying beliefs, assumptions, values, and ways of interacting that contribute to the unique social and psychological environment of an organization.6 Beginning with the Chief Executive and then down, leaders are key to the creation, maintenance, and communication of organizational culture.

Figure 2: Successful execution within an organization occurs when Leadership, Strategy, and Culture align.

Secretary of the Navy, Cybersecurity Readiness Review, 4 arch 2019; page 10

Business Culture & Risk Management

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate *governance* structures for managing such risk;
- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

NIST Special Publication 800-39 Managing Information Security Risk Organization, Mission, and Information System View, pg. 1

Risk Management

a. Cybersecurity Risk Management. Managing cybersecurity risks is a complex, multifaceted undertaking that requires the involvement of the entire organization, from senior leaders planning and managing DoD operations, to individuals developing, implementing, and operating the IT supporting those operations. Cybersecurity risk management is a subset of the overall risk management process for all DoD acquisitions as defined in Reference (at), which includes cost, performance, and schedule risk associated with the execution of all programs of record, and all other acquisitions of DoD. The risk assessment process extends to the logistics support of fielded equipment and the need to maintain the integrity of supply sources.

https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/850001_2014.pdf

Evaluation - strategies

- Who will conduct?
- Consistency
- Questionnaire
- Site Visit
- Interviews
- Attend training
- Evaluate – assess the next tier
- As an alternative
  - Ask about their supply chain
  - How do they identify subcontractors/suppliers?
  - How do they vet these companies?

Apply DoD's perspective

Supplier Risk

Supplier Risk Score is an overall score using 3-years of supplier performance information (PI) data designed to calculate and identify supplier risk by calculating a single overall numerical score. The Supplier Risk Score is derived by using ten identified risk factors and adjusting based on age, number of contracts, and record weight. The final scores are ranked against one another to provide a color ranking based on a 5-color rating system.

The Supplier Risk Report does not consider if the vendor is on DLA's Qualified Manufacturer/Producer List, so it may be different than the one displayed when performing a procurement Risk Analysis report.

https://www.sprs.csd.disa.mil/report-supplierrisk.htm

Understand – First Principles

- *…to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.*
- *The CMMC implementation will provide the Department with an ability to illuminate the supply chain, for the first time, at scale across the entire DIB sector.*

Concerns – past & current

Traditional

- Quality
- Capacity
- Delivery – on-time
- Price
- Flexibility
- FAR Part 9 – Responsible
  - General Standards

Evolving

- Cyber
- Location
- Down-stream processes
- Supply base
- Ownership
- Investors

Trusted Capital

https://www.acq.osd.mil/tc/

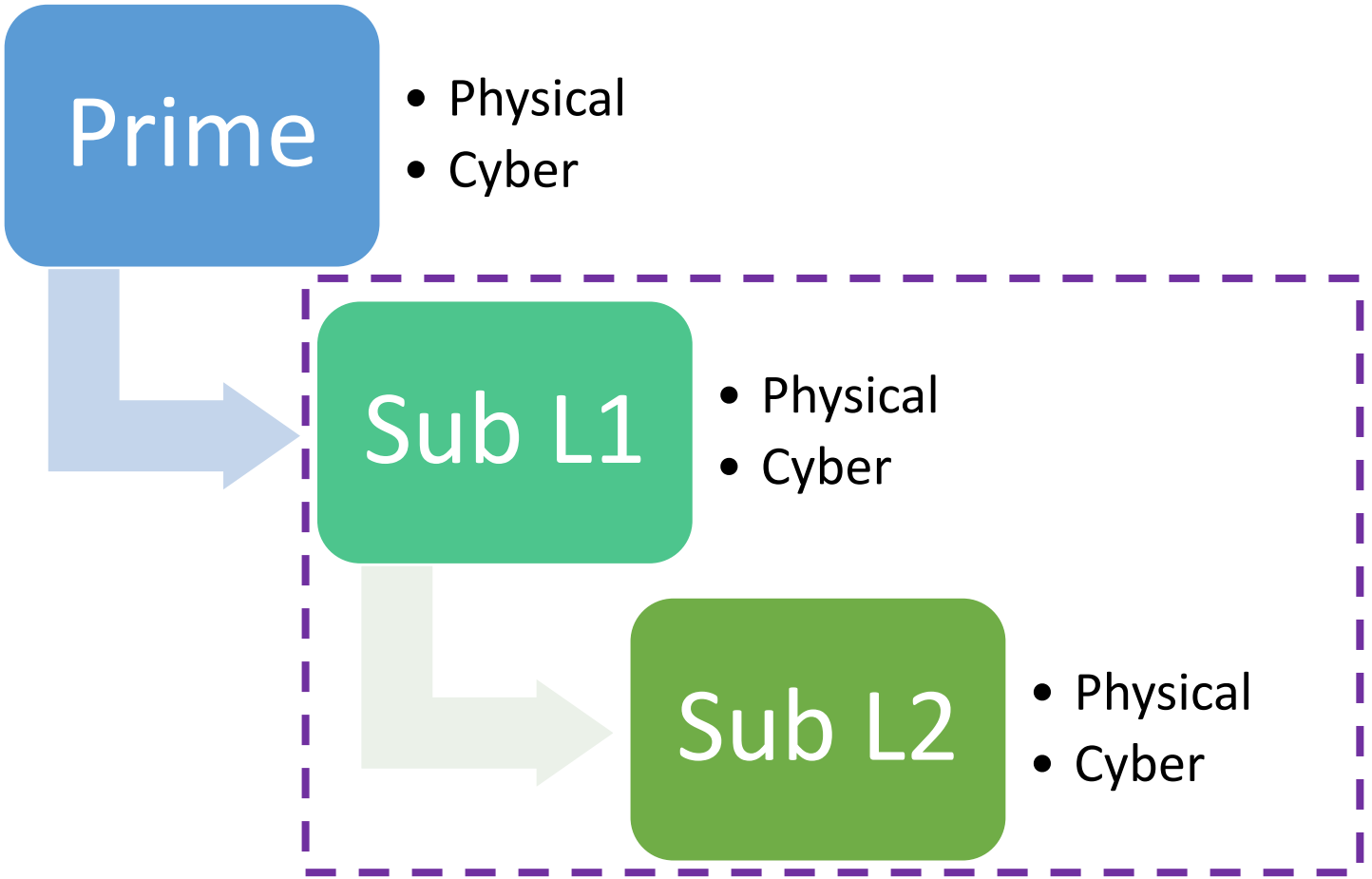
Thanks to Our Partners

dun & bradstreet

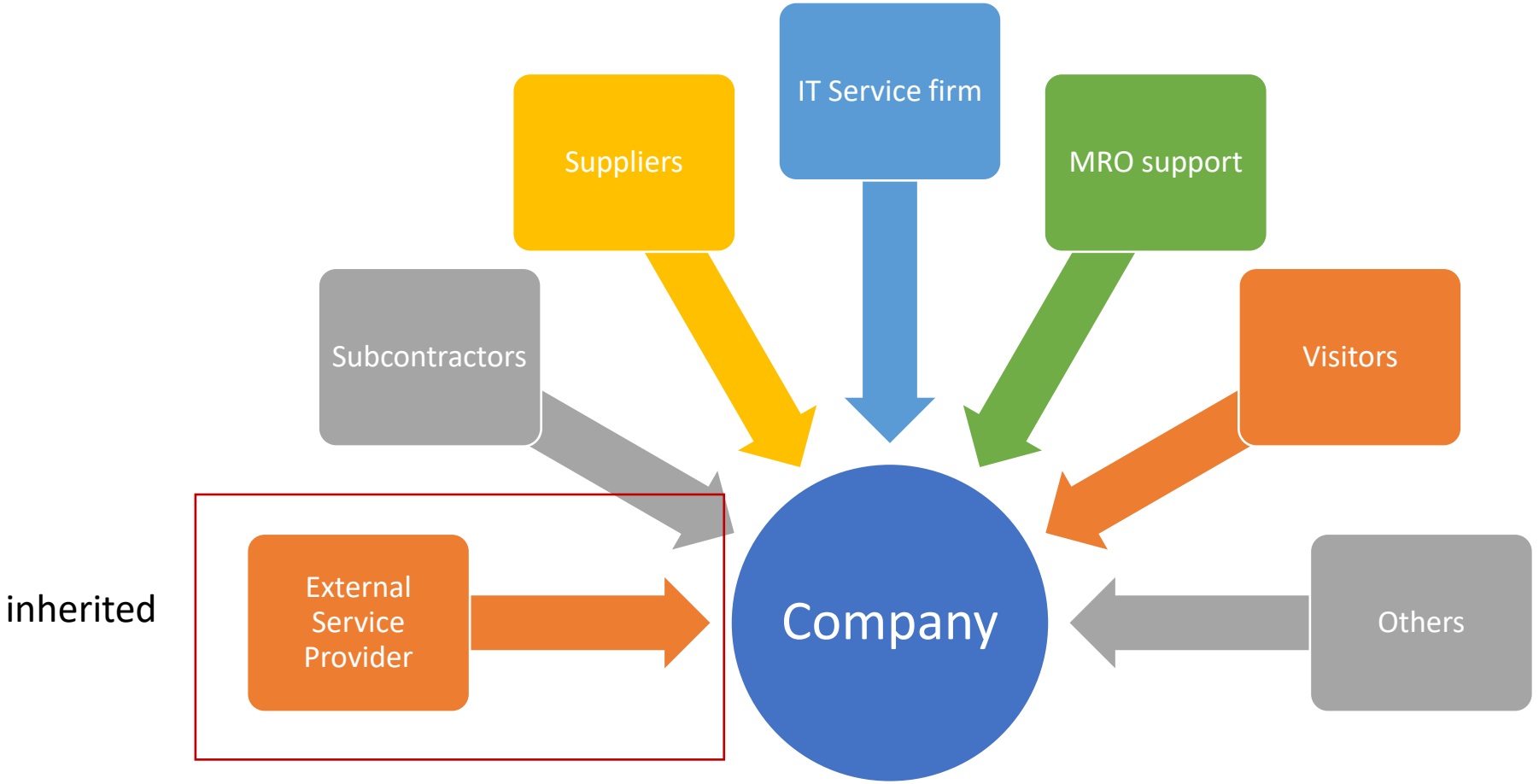
GROWING RELATIONSHIPS THROUGH DATA

https://cmmcab.org/

Map & Understand Supply Chain



Managing Relationships and Information Security/flow



Determine – “who are you doing business with?”

- Current security philosophy/posture – Basic (required) or better* (enhanced)
- Designation of Company Information Security Officer or equivalent
- Ownership, Control, Foreign Investors
- Keeping current
- References use – maintained
- Determination of Governmental Purpose
- Minimizing access
- Handling of Export-Controlled information
- Awareness and Management of CTI
- Understanding of requirements – details
- Storage capability
- Ability to decontrol – destroy various information types (disposition)
- Publication requirements/procedures

Assess corporate culture & philosophy

- Leadership – engaged, interested
- Memberships – ISAC, other industry group
- Efforts mechanical?
- Assess strengths – weaknesses
- Internal business communications
- Logging, logs, analysis, investigation, internal reporting

Create an Initial Assessment

- Year first registered in SAM
- Date projected for achieving 110
- Date of Assessment
- Number of subsequent Assessments
- % increase in Summary Score
- Uses the Cloud?
- Third party IT support?
- Types of information handled/processed
- Show example of a “dummy” email forwarding CUI
- Review sensitive information Transmittal Log

Identify general Risk Vectors

- Facility
- Network
- Policies
- Staff
- Subcontractors
- Suppliers
- Vendors
- Visitors

Determine what plans are maintained?

- Business Continuity
- Data protection
- Data storage
- Data sharing
- Data marking
- Data type inventory
- Data usage agreement – internal
- Data type – access list
- Information security – exercise plan
- Information security – training requirements

252.204-7000 Disclosure of Information.

As prescribed in 204.404-70 (a), use the following clause:

DISCLOSURE OF INFORMATION (OCT 2016)

(a) The Contractor shall not release to anyone outside the Contractor's organization any unclassified information, regardless of medium (e.g., film, tape, document), pertaining to any part of this contract or any program related to this contract, unless—

(1) The Contracting Officer has given prior written approval;

(2) The information is otherwise in the public domain before the date of release; or

204.404-70 Additional contract clauses.

(a) Use the clause at 252.204-7000 , Disclosure of Information, in solicitations and contracts when the contractor will have access to or generate unclassified information that may be sensitive and inappropriate for release to the public.

(b) Use the clause at 252.204-7003 , Control of Government Personnel Work Product, in all solicitations and contracts.

Test for familiarity with requirements

52.204-21 Basic Safeguarding of Covered Contractor Information Systems.

As prescribed in 4.1903 , insert the following clause:

BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) *Definitions.* As used in this clause–

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

Federal contract information 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.

Additionally -

(1) The DoD originator or authorized CUI holder must ensure a prepublication and security policy review is conducted, pursuant to the standard DoD Component process, before CUI is approved for public release, which includes publication to a publicly accessible website.

DoDI 5200.48, March 6, 2020; page 13; 3.3 a (1)

(m) Subcontracts. The Contractor shall—

- (1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties.

The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

5.3. REQUIREMENTS FOR DOD CONTRACTORS

a. Whenever DoD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle, in whole or part, and mark such documents, material, or media in accordance with this issuance.

b. Whenever the DoD provides CUI to, or CUI is generated by, non-DoD entities, protective measures and dissemination controls, including those directed by relevant law, regulation, or government-wide policy, will be articulated in the contract, grant, or other legal agreement, as appropriate.

c. DoD contracts must require contractors to monitor CUI for aggregation and compilation based on the potential to generate classified information pursuant to security classification guidance addressing the accumulation of unclassified data or information. DoD contracts shall require contractors to report the potential classification of aggregated or compiled CUI to a DoD representative.

d. DoD personnel and contractors, pursuant to mandatory DoD contract provisions, will submit unclassified DoD information for review and approval for release in accordance with the standard DoD Component processes and DoDI 5230.09.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf, page 32

DoD Guidance

- Requiring delivery of the contractor's system security plan (or extracts thereof)
- Requiring the contractor to identify known Tier 1 Level suppliers
- Requesting the contractor's plan to track flow down of covered defense information and to assess DFARS clause 252.204-7012 compliance of known Tier 1 Level suppliers.

https://www.acq.osd.mil/dpap/pdi/cyber/docs/Guidance_for_Assessing_Compliance_and_Enhancing_Protections.pdf

252.204-7020 Paragraph (g) Subcontracts

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

Supplier agreements – presence & use of

- What notification requirements should be required?
  - Key staff –
    - Move/departure/hires
  - Interest in purchase/investing
  - Unusual requests for information – external – non-federal
  - Changes in key supplier/subcontractor
  - Changes in cyber-security status – supplier/subcontractor
  - Requirement for periodic testing of cyber-incident response plan
  - Maintenance of an active DoD Medium Assurance Certificate
  - Acknowledgement of the ability to capture a forensic network image IAW DFARS 252.204-7012

Formally adopt plans & policies

- Board approval
- CEO/President date, signature, revision
- Establish controls
  - Change
  - Version
  - Distribution
  - Responsibility
  - Edits/corrections/updates
  - Test – it sounds good; does it work?
  - List of effect pages - LOEP

Significant questions

- How do you know?
- Can you show?
- Do you have documentation?
- What triggers an update?
- Are violations tracked?
- Do you have policies and procedures?
- How are staff members informed?
- What type of training is conducted?
- How is network traffic monitored?
- Does the company have cyber insurance?
  - What kind(s)?

Develop a Risk Profile

- Information type
  - JCP | ITAR | CUI | Other
- Review of company web site
- Review of select policies
- Performance metrics – quality / on-time
- Leadership involvement
- Responsiveness
- Training documentation
- Turn-over key positions

Determine KPI's of current efforts

- Date performed – Date last update
- Number of items (5) - 42
- Number of items (3) - 14
- Number of items (1) - 51
- Estimated completion date – item value
- Review project plan –
  - Not item number & status
  - Workable plan – status: draft, intermediate, final

5 Questions CEOs Should Ask About Cyber Risks

1) How Is Our Executive Leadership Informed About the Current Level and Business Impact of Cyber Risks to Our Company?
2) What Is the Current Level and Business Impact of Cyber Risks to Our Company? What Is Our Plan to Address Identified Risks?
3) How Does Our Cybersecurity Program Apply Industry Standards and Best Practices?
4) How Many and What Types of Cyber Incidents Do We Detect In a Normal Week? What is the Threshold for Notifying Our Executive Leadership?
5) How Comprehensive Is Our Cyber Incident Response Plan? How Often Is It Tested?

Utilize appropriate references (partial list)

Defend Against Cyber Attack

- DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA)
- DoDI 8310.01, Information Technology Standards in the DoD
- DoDI 8500.01, Cybersecurity
- DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
- DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- DoD 8530.01-M, "DoD Computer Network Defense Service Provider Certification and Accreditation
- DoDI 8540.01, "Cross Domain (CD) Policy
- Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings

https://dodcio.defense.gov/library/

Cloud Security

After a year when digital transformation took a quantum leap at most enterprises and remote work exploded, it's no surprise that the majority of enterprise workloads are now running in cloud-based infrastructure as a service (IaaS) and platform as a service (PaaS) offerings.

This is creating a whole new set of security challenges around managing access to your organisation's infrastructure across multiple cloud platforms—with all the various identities and configurations they bring. Studies have shown this is where security failures happen—when the combinations of identities, access entitlements and privileges break down; Gartner forecasts that will account for about three-quarters of security incidents in the cloud by 2023.

https://cloudcomputing-news.net/news/2021/mar/10/a-guide-to-privileged-access-management-the-doorman-for-the-cloud/
https://www.forbes.com/sites/forbestechcouncil/2020/11/30/dont-underestimate-the-business-risk-of-cloud-entitlements

Perimeter Defense & the Cloud

“We use the cloud”

Identity is the new perimeter

When identity becomes the security perimeter —as it does in the cloud —then privileged access is even more crucial. Not every account needs an all-access pass to the VIP rooms in your environment, not even admins. So the ability to grant granular access permissions and privileges based on who has access, who really needs it and when, is important.

If you have hundreds or thousands of privileges in the cloud and only one percent of them are in use, this leaves an enormous attack surface exposed to the bad guys. The cloud gets points for scalability and flexibility, but that means that services are constantly growing, and spinning off more identities and privileges left open to attack.

https://cloudcomputing-news.net/news/2021/mar/10/a-guide-to-privileged-access-management-the-doorman-for-the-cloud/

JCP

- Is the current certification valid?
- Into the regulation - DoDI

Don’t assume

5.4.2. The requested data are judged to be unrelated to the purpose for which the qualified U.S. contractor is certified. When release of technical data is denied in accordance with this paragraph, the controlling DoD office shall request additional information sufficient to explain the intended use of the requested data and, if appropriate, request a new certification (see paragraph 3.2., above) describing the intended use of the requested data; or

DoDD 5230.25, November 6, 1984; Change 2, 10/15/2018 - JCP

Question -1

- A contractor received its CMMC certification a little over two years ago. Based upon information provided by this contractor, they have not previously handled CUI or similar sensitive information.
- Q – Since they have the proper CMMC Level certification can you share the information with them?
- Q – Are there any concerns?
- Q – What additional actions should be taken?

Question - 2

- What is the fewest number of questions that need to be asked to understand this company's cybersecurity capabilities?
- What would you use as a guide and why?
- What does it mean if they outsourced their CMMC?
- What does it mean if they are overly reliant upon third-party IT services?
- What impact (risks) might this have?
- Are these risks manageable?

Questions - 3

- How might the company's location be of concern?
- Is the company's turn-over rate of concern? – why?
- How are the company's plans, policies and procedures maintained?
- What are some of the key ideas you would expect to hear concerning how do they vet members of their supply chain?
- How is information managed – receipt/storage/sharing
- When was staff training last conducted? What were the topics?
- A staff member receives an email with an attachment from a prospective customer upon opening the attachment, the staff member sees that the drawing is identified as Distribution Statement D. How will this issue be managed?

Who should be interviewed?

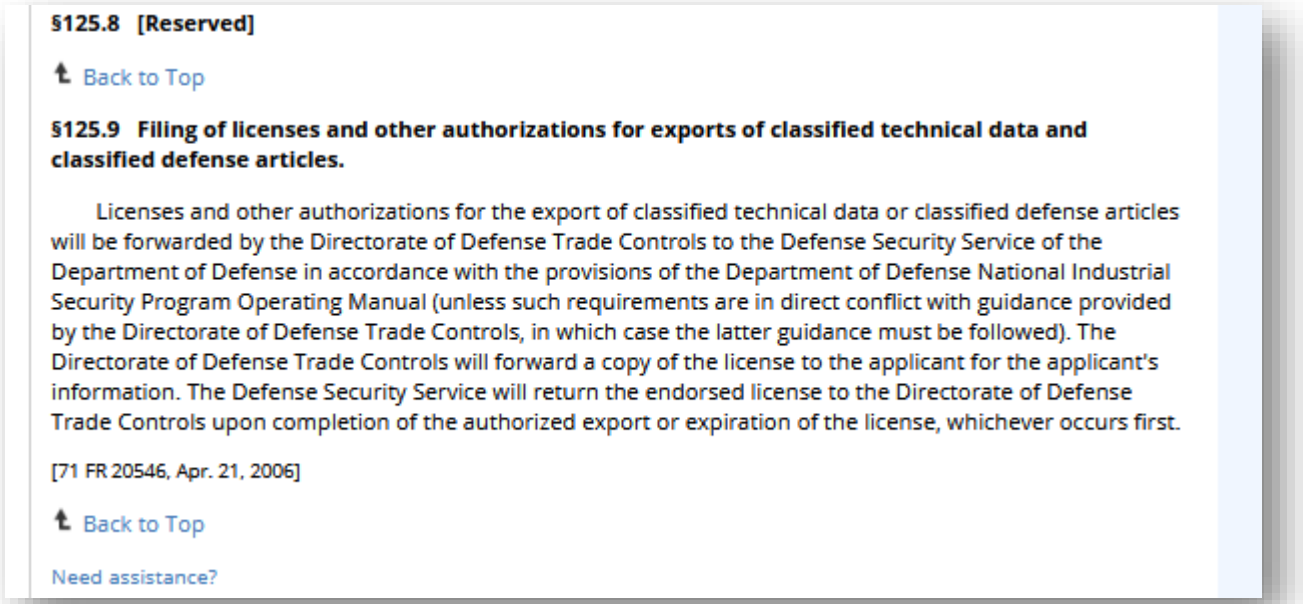
- Which staff members – staff positions should be interviewed?

Validate references

[1] Canadian contractors may be qualified in accordance with this Directive for technical data that do not require a license for export to Canada under section 125.12 of the ITAR (reference (g)) and section 379.4(d) and 379.5(e) of the EAR (reference (f)) by submitting an equivalent certification to the U.S. Department of Defense.

[2] This does not require a contract with or a grant from the U.S. Government.

Change 2, 10/15/2018



§125.8 [Reserved]

Back to Top

§125.9 Filing of licenses and other authorizations for exports of classified technical data and classified defense articles.

Licenses and other authorizations for the export of classified technical data or classified defense articles will be forwarded by the Directorate of Defense Trade Controls to the Defense Security Service of the Department of Defense in accordance with the provisions of the Department of Defense National Industrial Security Program Operating Manual (unless such requirements are in direct conflict with guidance provided by the Directorate of Defense Trade Controls, in which case the latter guidance must be followed). The Directorate of Defense Trade Controls will forward a copy of the license to the applicant for the applicant's information. The Defense Security Service will return the endorsed license to the Directorate of Defense Trade Controls upon completion of the authorized export or expiration of the license, whichever occurs first.

[71 FR 20546, Apr. 21, 2006]

Back to Top

Need assistance?

Preventing Uncontrolled Foreign Access

4.2. Because public disclosure of technical data subject to this Directive is tantamount to providing uncontrolled foreign access, withholding such data from public disclosure, unless approved, authorized, or licensed in accordance with export control laws, is necessary and in the national interest. Unclassified technical data that are not governed by this Directive, unless otherwise restricted, shall continue to be made available to the public as well as to State and local governments.

DoDD 5230.25, November 6, 1984; Change 2, 10/15/2018 – JCP

Network Logs

- What logs are used by the company?
- How were they selected?
- What is there granularity?
- How frequently are they reviewed?
- Who conducts the review?
- What training have they received?
- Are there any software tools used to support these efforts?
- How is this information used?
- With whom is this information shared?

Controlled Technical Information

c. CTI compiled or aggregated may become classified. Such classified CTI is subject to the requirements of the National Industrial Security Program, which has different requirements than Section 252.204-7012 of the DFARS for unclassified CTI.

(1) CTI is to be marked with one of the Distribution Statements B through F, in accordance with DoDI 5230.24.

DoDI 5200.48, March 6, 2020, page 20

Identify and validate requirements

3.6. GENERAL DOD CUI PROCEDURES

b. In accordance with this issuance, every individual at every level, including DoD civilian and military personnel as well as contractors providing support to the DoD pursuant to contractual requirements, will comply with the requirements in Paragraph 3.6.f of this issuance for initial and annual refresher CUI training.

https://www.dodcui.mil/Portals/109/Documents/Policy%20Docs/DoDI%205200.48%20CUI.pdf; pages 17-18
DoDI 5200.48, March 6, 2020

Inquire about

(1) Implementation activities.

(2) Training statistics.

(3) Incident management.

(4) Implementation and sustainment costs.

(5) Self-inspection activities.

- DoD activities are required to submit a CUI Implementation Annual Report.
- Does it make sense for your vendors to do so as well?

DoDI 5200.48, March 6, 2020; page 17

UPCOMING TRAINING - EVENTS

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

CYBER FRIDAY LIVE WEBINAR SERIES

Mar 19, 2021 Managing Vendor Risk

April 16, 2021 Your Cyber Plan Cannot Be Static – Here's Why!

April 30, 2021 Testing and Strengthening Your Cyber-Defenses Using Exercises

May 14, 2021 Corporate Acquisition, Insider threats, or Strategic Investments – All Threats to Consider

Register at: https://www.wispro.org/faqs/what-is-wpis-current-cyber-friday-webinar-schedule/

PRESENTED BY

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
Cyber Friday

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

ACQUISITION HOUR LIVE WEBINAR SERIES

- March 23, 2021

  The SBA 8(a) Certification Program and Small Disadvantaged Businesses (SDB)
  CLICK HERE for additional information
  Presented by Shane Mahaffy, U.S. Small Business Administration

- March 24, 2021

  Acquisition Hour: Using the New FPDS and Desktop Tools to Analyze Federal Procurement Data
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute

- April 6, 2021

  Acquisition Hour: Intellectual Property for Government Contractors & Subcontractors & the STTR/SBIR Stakeholder
  CLICK HERE for additional information
  Presented by Laura Grebe, Husch Blackwell

- April 13, 2021

  Acquisition Hour: Veterans' Small Business Certifications – Federal and State
  CLICK HERE for additional information
  Shane Mahaffy, U.S. Small Business Administration and Tondra Davis, State of Wisconsin Department of Administration

- April 20, 2021

  Acquisition Hour: Introduction to Certifications Available to Minority Owned Businesses
  CLICK HERE for additional information
  Tondra Davis, Wisconsin Department of Administration; Madalena Maestri, Wisconsin Department of Transportation; Benjamin Blanc, Wisconsin Procurement Institute

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
ACQUISITION HOUR

…More at wispro.org/events

8th Annual FAR Evening Study Sessions

Presented by the National Contract Management Association (NCMA Wisconsin) and WPI

February 2, 2021	Intro & FAR Part 16	**March 2, 2021**	FAR Parts 19-29
February 9, 2021	FAR Parts 1-4	**March 9, 2021**	FAR Parts 30-33
February 16, 2021	FAR Parts 5-12	**March 16, 2021**	FAR Parts 34-41
February 23, 2021	FAR Parts 13-18	**March 23, 2021**	FAR Parts 42-53

Register at: https://www.wispro.org/wpis-2021-far-evening-study-sessions-schedule/

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

WPI Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

2021 FAR Up Close Series

February 10, 2021	Overview of the FAR
February 17, 2021	FAR Regulations and Clauses on Subcontracting
March 3, 2021	FAR Regulations and Clauses in Commercial Items
March 10, 2021	FAR and DFARS Regulations and Clauses in Manufacturing Contracts
March 17, 2021	FAR Regulations and Clauses in Federal Service Contracts
April 7, 2021	FAR Clauses in Federal Construction Services
April 14, 2021	FAR Regulations for Procurement of Architect Engineer Services

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
FAR Up Close

Register at: https://www.wispro.org/wpis-2021-far-up-close-schedule/

CYBERSECURITY – UPDATE – DECEMBER 2020

- CMMC -
  - Implementation continues
  - Pathfinder contracts to be announced soon – article, Dec 1, 2020
    - CMMC requirements will be included
  - Full implementation expected by Oct 2025
- New clauses and requirements –
  - DFARS 252.204-7019
  - DFARS 252.204-7020 – applies to contracts subject to 252.204-7012
    - With few exceptions, these requirements apply to all Primes and Subcontractors
    - Consistent with philosophy shift of self-attest to verifiable
    - Three levels – Base – self-performed , Medium & High - DCMA

252.204-7020 – BASIC ASSESSMENT

- Requires
  - System Security Plan(SSP)
  - Plan of Action – with dates for outstanding items
  - Basic Assessment
- Six elements uploaded to Supplier Performance Risk System (SPRS)
  1. System Security Plan name (if more than one system is involved)
  2. Brief description of Plan Architecture
  3. CAGE code associated with SSP
  4. Date Assessment performed
  5. Summary Score
  6. Date a score of 110 to be achieved

CURRENT CYBER REQUIREMENTS

- FAR 52.204-21 – Federal Contract Information
- DFARS 252.204-7012
- Requirements cited in solicitation/contract

Need assistance – please contact Marc Violante from WPI at marcv@wispro.org or 920-456-9990

CONTINUING PROFESSIONAL EDUCATION

CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

Cyber Friday

PRESENTED BY

Wisconsin Procurement Institute (WPI)
www.wispro.org

Marc Violante
Wisconsin Procurement Institute (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226