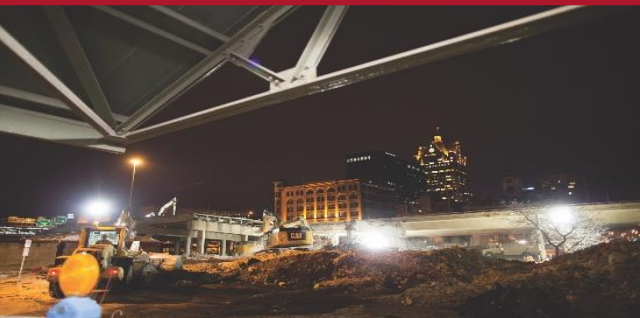




**HOW THE CYBERSECURITY MATURITY MODEL
CERTIFICATION (CMMC) WILL IMPACT YOUR BUSINESS**
ACQUISITION HOUR WEBINAR

February 5, 2020



WEBINAR ETIQUETTE

PLEASE

- Log into the GoToMeeting session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the CHAT option to ask your question(s).
 - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

ABOUT WPI SUPPORTING THE MISSION

**Celebrating 32 Years of
serving Wisconsin Business!**



Assist businesses in creating, developing and growing their sales, revenue and jobs through Federal, state and local government contracts.

- **INDIVIDUAL CONSELING** – At our offices, at clients 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

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*

▪ OSHKOSH

- *Fox Valley Technical College*
- *Greater Oshkosh Economic Development Corporation*

▪ EAU CLAIRE

- *Western Dairyland*

▪ MENOMONIE

- *Dunn County Economic Development Corporation*

▪ LADYSMITH

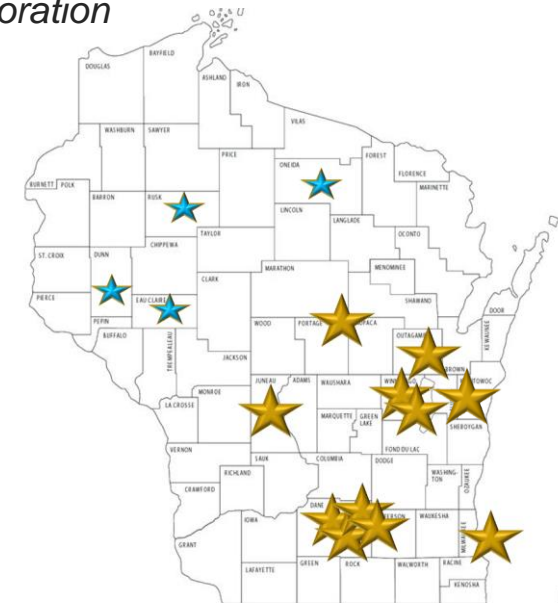
- *Indianhead Community Action Agency*

▪ RHINELANDER

- *Nicolet Area Technical College*

▪ GREEN BAY

- *Advance Business & Manufacturing Center*





Search ...

BLOG SERVICES ABOUT **CLIENT PORTAL** SPONSORSHIP CONTACT



- EVENT CALENDAR
- FEDERAL GOVERNMENT
- STATE & LOCAL GOVERNMENT
- GRANTS
- SUCCESS & AWARDS
- FAQS



www.wispro.org

UPCOMING EVENTS

- WED 21** Acquisition Hour: Government Property Management for Federal Contractors and Subcontractors
August 21 @ 12:00 pm - 1:00 pm
- THU 22** Advancing Cybersecurity in the Industry, Energy, Water Nexus – Oshkosh, WI
August 22 @ 9:00 am - 3:00 pm
Oshkosh WI
- THU 22** NDIA Great Lakes Chapter 10th Anniversary – Milwaukee, WI
August 22 @ 12:30 pm - 7:30 pm
Brookfield Wisconsin
- SEP 11** Acquisition Hour: The End of the Fiscal Year is Here – What is Hot and What is Not
September 11 @ 12:00 pm - 1:00 pm

[View More...](#)

CURRENT OPPORTUNITIES (1)

GET STARTED WITH THE BASICS

Questions & answers on how to get started.

[GET STARTED](#)

SIGN-UP FOR OUR NEWSLETTER

Stay up-to-date with the latest WPI news.

[SIGN UP](#)

HAVE A QUESTION? WE'RE HERE TO HELP.

One of our staff of experts is available to answer your questions.

[GET HELP](#)

CMMC

How the Cybersecurity Maturity Model Certification (CMMC) Will Impact Your Business

Marc N. Violante

Wisconsin Procurement Institute

February 5, 2020

CMMC – DoD's perspective

The CMMC is outlined for our program managers in DOD instruction 5000.CSA, the new adaptive acquisition framework. The CMMC is also influencing program protection plans and DoDI 80 -- 8500.01 and 8510.01, which both focus on the protection of I.T. and information systems.

The CMMC establishes security as the foundation to acquisition and combines the various cyber-security standards into one unified standard.

Department of Defense Press Briefing by Undersecretary of Defense for Acquisition and Sustainment
Ellen M. Lord
Oct. 18, 2019

2/5/2020

Slight Change



**Without a Secure Foundation
All Functions are at Risk**



DISTRIBUTION A. Approved for public release

2/5/2020

2

The desired end state

- build
 - a cyber-safe,
 - cyber-secure and
 - cyber-resilient
- } defense industrial base

Cause and Effect

- “Adversaries know that in today's great power competition environment, information and technology are both key cornerstones and -- and attacking a sub-tier supplier is far more appealing than a prime.
- “ We know that the adversary looks at our most vulnerable link, which is usually **six, seven, eight levels down in the supply chain**. So right now, there are a number of primes who have come up with some ideas about how to more cost-effectively accredit small and medium businesses.”
- “CMMC is a critical element of DOD's overall cybersecurity implementation. ”

Ellen M. Lord, Assistant Secretary of Defense for Acquisition, Press Briefing transcript, January 31, 2020

2/5/2020

CMMC – in general

- 5 Levels
- Companies will determine/select an appropriate level for them
 - Selection keyed to prime's and/or customer's need
 - Level will be indicated in DoD solicitations
- **All companies will be certified** – no exemptions
 - At a minimum companies will certify to Level 1 ~ FAR 52.204-21
 - Level 3 – CUI
 - Levels 4 and 5 – small number of companies dealing with highly sensitive CUI
- Periodic recertifications will be required

CMMC - recertification

- Levels 4 & 5 – annually
- Level 3 – every two years
- Levels 1 and 2 – every three years

Comments by Ms. Katie Arrington during Exostar Webinar

2/5/2020

CMMC Domains

- The CMMC model consists of 17 domains
 - The majority originate from FIPS Standard 200
 - NIST 800-171
- The CMMC model also includes three domains –
 - Asset Management (AM)
 - Recovery (RE)
 - Situational Awareness (SA)

Figure 4 – CMMC Domains



The ink is still wet!

Current milestones

- CMMC Accreditation Board – established – January 2020
- CMMC V1.0 issued – Friday, January 31, 2020
 - See: <https://www.acq.osd.mil/cmmc>
 - Briefing slides
 - CMMC Model v1.0 pdf
 - References

CMMC A.B.– key players

- CMMC Accreditation Board – see: <https://www.cmmcab.org>
- Board – 17 members – 15 filled (Tuesday, Feb 4, 2020)
- Assessors – will perform the onsite review
- C3PAO –
 - the organizations where licensed assessors will come together hone their skills and register their licenses.
 - C3PAO's will require certification by CMMC A.B.
- Trainers – trainers will train the assessors (~ 10,1000+)
- Staff

CMMC A.B. – currently seated board

1. Chairman, Ty Schieber, University of Virginia, Darden School Foundation
2. Director, Akin Akinbosoye, Manufacturing x Digital (MxD)
3. Director, Carl Anderson, HITRUST
4. Director, Mark Berman, FutureFeed
5. Director, Wayne Boline, Raytheon
6. Director, Jeff Dalton, Broadsword Solutions
7. Director, Nichole Dean, Accenture Federal Services
8. Director, Regan Edens, DTC Global
9. Director, James Goepel, Fathom Cyber, LLC
10. Director, Chris Golden, Third-Party Risk Management
11. Director, Karlton Johnson, Delaine Strategy Group, LLC
12. Director, Richard Klodnicki, Aereti, Inc.
13. Director, Tim Rudolph, 3d Millennium Group
14. Director, Ben Tchoubineh, Phoenix TS
- 15.
16. Director, John Weiler, IT Acquisition Advisory Council (IT-AAC)
17. TBD

In their (CMMC A.B.) own words – re: C3PAO

What we don't know...

We don't know when you will be able to register to become an official C3PAO. Think Q2 2020, but there is much work to complete before that registration and certification process will be available.

We don't know yet know the rules for what it takes to be a C3PAO in good standing.

We don't know the fees or details associated with the process. The CMMC-AB is a nonprofit. Our fees will reflect the costs of providing an independent, national organization with a leading-edge customer experience.

But wait. We are just getting started.

Come back here often for detail and sign up below for alerts and emails.

There is much to come, we will provide information as we build it.

...yet.

Prospective Assessors

- **Where can I get trained as an Assessor?**
 - **Since training does not yet exist**, there are no locations approved to provide certified CMMC Assessor Training.
- **When do you expect Assessor training to be available?**
 - The DoD has indicated that it will provide initial training guidance to the CMMC-AB in the first quarter of 2020. We expect to work diligently from those materials to make training available as quickly as is practical, while balancing the need for quality, consistency, and speed.

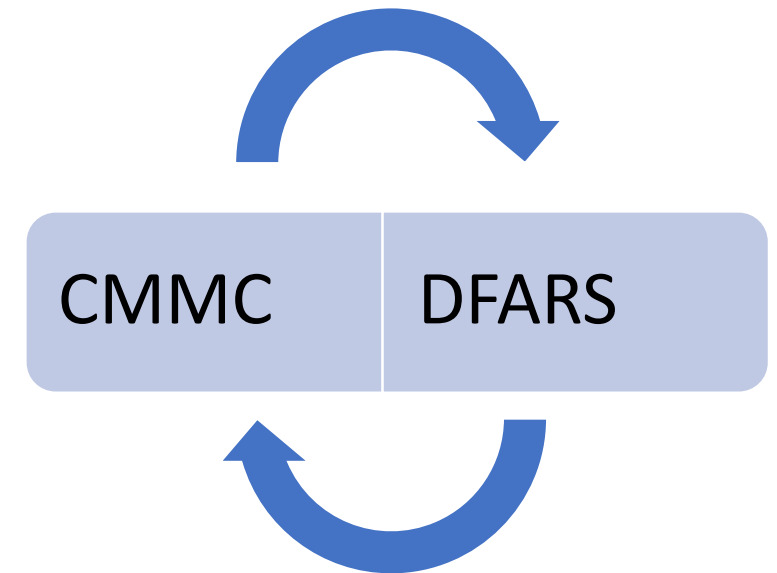
Prospective C3PAOs

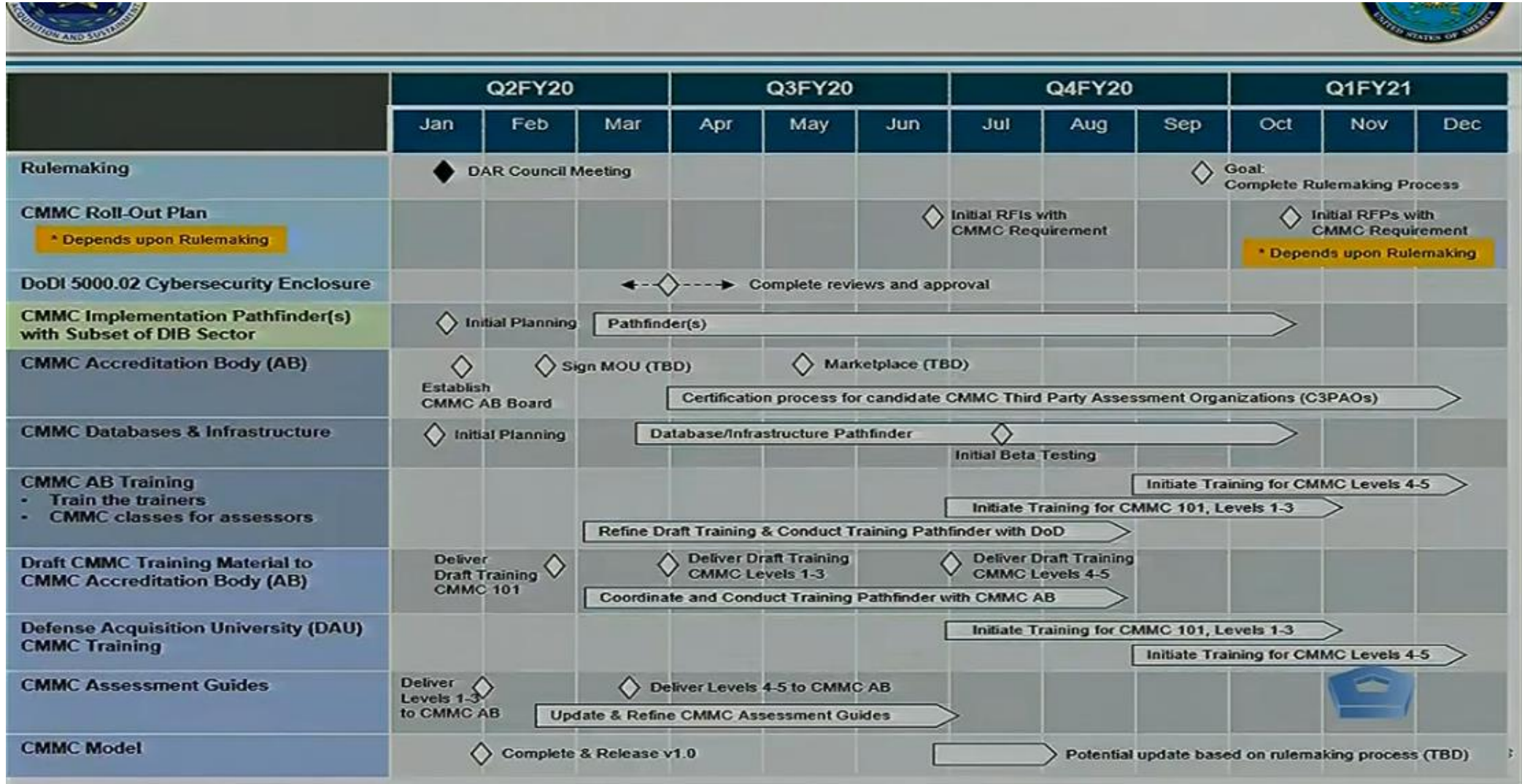
- **My company already performs assessments under other standards/frameworks. Can we start offering CMMC assessments?**
 - The CMMC Standard is not yet finalized and no Assessors or C3PAOs are formally accredited or certified by the CMMC-AB. Therefore, it is currently inappropriate for any Assessor or C3PAO to claim to provide formal CMMC assessments that will meet the requirements for a DoD contract.
- **What about pre-assessments?**
 - To be clear, offering pre-assessments or consulting using the most current draft of the standard is acceptable and encouraged. **However, it is not currently appropriate for any vendor to offer a formal CMMC assessment claiming that is authorized by the CMMC-AB.**



Time Line

- Late spring/early summer timeframe to complete a new defense acquisition regulation, a new Defense Federal Acquisition Regulation, or DFAR.
- CMMC requirement in selected RFIs [request for information] in the June 2020 timeframe
- Corresponding RFPs [request for proposals] in September 2020 time frame, where CMMC standards will be required at the time of contract award.





Timeline charge from January 31, 2020 Press Briefing

2/5/2020

Major Milestones

- The department is working with the military services and agencies to identify candidate programs that will implement the CMMC requirements during the F.Y. 2021 through F.Y. '25 **phased rollout**.
- All **new** DOD contracts will contain the CMMC requirements, **starting in F.Y. '26**.
- Consequently, organizations working with the DOD will need a CMMC certification **within the next five years**.

Target numbers – roll out (pathfinder projects)

- Q: Is there a target number for how many initial RFIs will be rolled out this summer with CMMC? And then, will that be a sort of deliberate mix of a percentage of Level 3, Level 4, Level 5?
- MS. ARRINGTON: We're targeting 10 RFIs and 10 RFPs this year.
- We figured that with each one, we've assumed that there would be 150 subcontractors along that in some capacity.
- So 10 contracts with 150 contractors per. And yes, it will be a mix. We'll have some CMMC Level 3, CMMC Level 1, and there may be one or two that have the 4 or 5 CMMC levels going out. But we are working those.

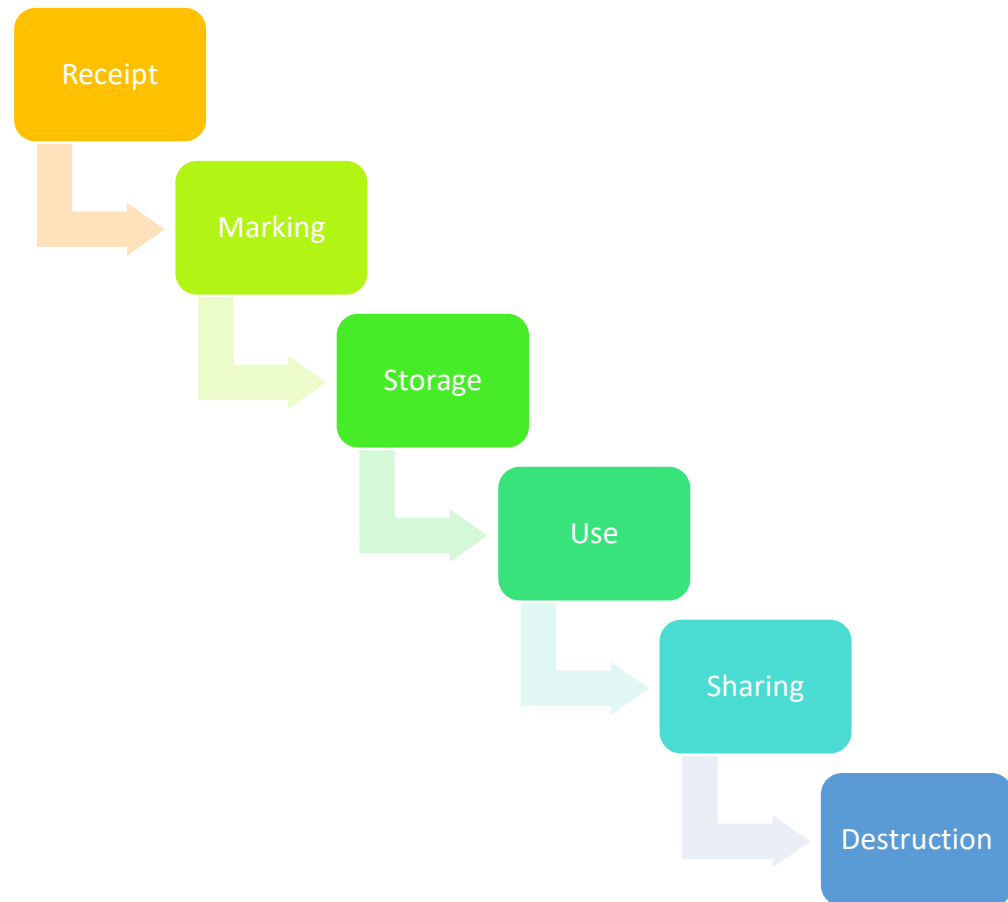
CMMC Marketplace

- Coming in the future
- Portal to schedule accreditation visits
- CMMC A.B. will establish requirement for candidate C-3PAOs and individual assessors.
- the CMMC will -- A.B. -- will provide updates on training classes, which are planned to start in early spring 2020.
- After the A..B. -- the CMMC A.B. certifies C-3PAOs, companies will be able to schedule CMMC assessments for specific levels through a CMMC marketplace portal.

Mindset = #1

- Protection efforts cannot be viewed as a managing a checklist.
- Recurring concept heard in DoD briefings
 - **Critical Thinking Skills** – with respect to cyber (mentioned not defined)
- CMMC is not a “thing” an endpoint a destination – given the evolving and growing cyber threats.
- A key and major step will be document/information management
 - Every document – piece of information needs to be categorized & marked
 - Public, Company Private, Customer Private, JCP, ITAR, CUI, FCI or other
 - Additionally, every employee needs to be (re)/trained on company procedures
- Implementation needs to integrate with other programs/information

Information – life cycle, general elements



- Auditing
- Awareness
- Controls
- ★ • Deliverables
- Information – source(s)
- Monitor – test
- Questions to KO, other
- Training
- ★ • Transmittal registry
- Update procedures

Paragraph (l) – 252.204-7012

(l) Other safeguarding or reporting requirements.

The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

Key Elements



Example – Integrated requirements (slide 1 of 3)

- **59 - Single Channel Ground & Radio System (1) – FBO Item**

- These items are the components of Interconnecting Group ON-373B/GRC; end system Single Channel Ground and Airborne Radio System (SINCGARS).

- The Government owns the technical data package (TDP) for the items. The TDPs will include drawings and Gerber files. The TDPs are subject to ITAR; refer to statement below.

- NOTE: The TDPs will NOT be released at this time.

- **INTERNATIONAL TRAFFIC IN ARMS REGULATIONS**

- The technical data package (TDP) for this item is subject to the International Traffic in Arms Regulations (ITAR). All technical documents for SINCGARS include but not limited to, test plans, test reports, drawings and specifications contains information that is subject to the controls defined in the International Traffic in Arms Regulation (ITAR). This information shall not be provided to non- U.S. persons or transferred by any means to any location outside the United States Department of State.

<https://www.fbo.gov/notices/0e1d8fa0af22781f98263ce131214688> - posted February 25, 2019

2/5/2020

Integrated example (slide 2 of 3)

- A company wishing to receive the TDPs must have an active status in the Defense Logistics Agency **Joint Certification Program (JCP)**.
- Once your company has been verified to have active status in JCP, we will upload the TDPs will be uploaded into AMRDEC Safe Access File Exchange (SAFE). You will then receive an e-mail from the AMRDEC SAFE site, <https://safe/amrdec.army.mil/safe/>, with a link to the package ID and a password.
- The TDPs may contain drawings in C4 format. Software to view C4 drawings is available for download through

<https://www.fbo.gov/notices/0e1d8fa0af22781f98263ce131214688> - posted February 25, 2019

Integrated example (slide 3 of 3)

- COVERED DEFENSE INFORMATION (CDI)

Note regarding DFARS 252.204-7008 and DFARS 252.204-7012: The Government not including or identifying CDI at this time does not constitute a lack of CDI for this solicitation/award

52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS
JUN/2016

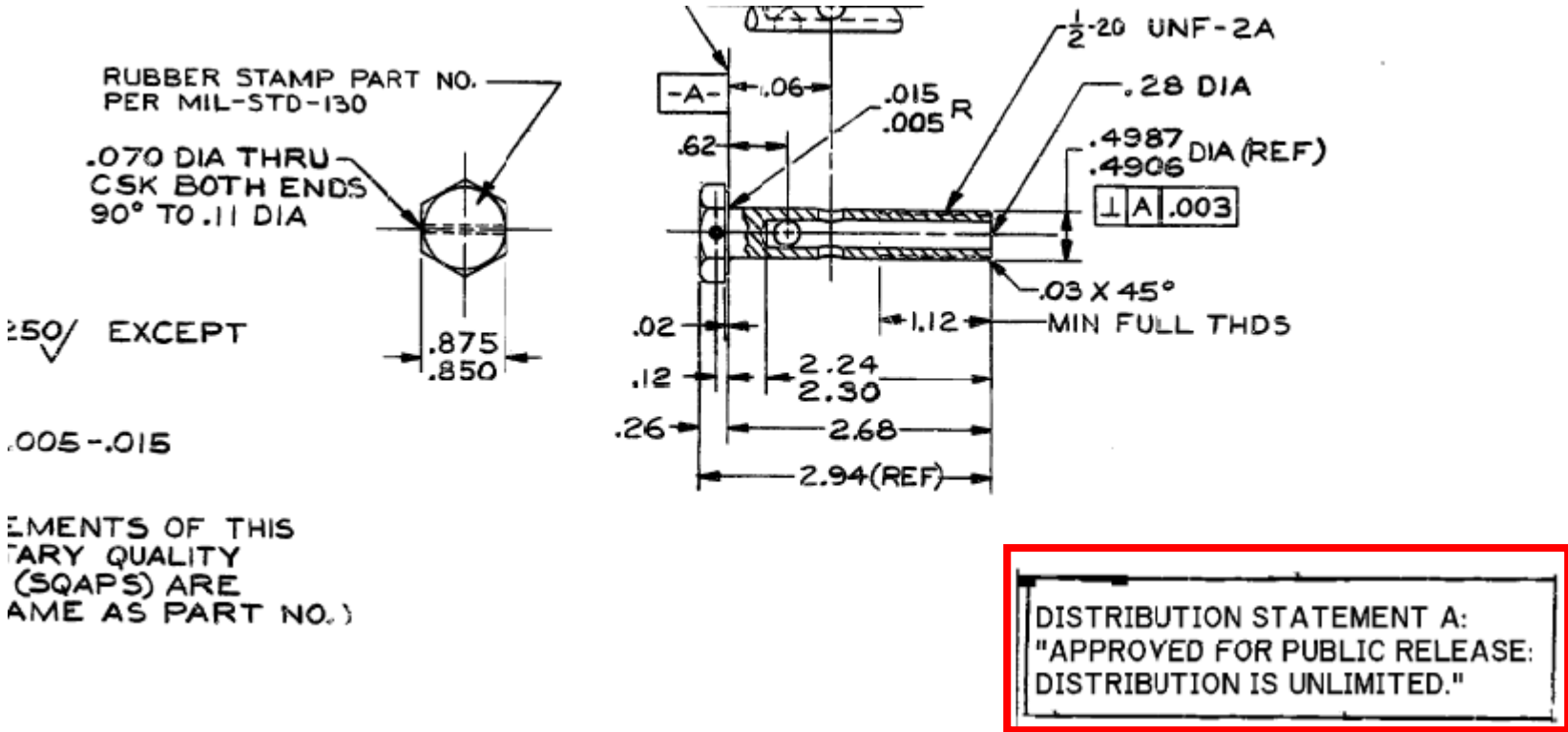
(a) Definitions. As used in this clause-

"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 Web sites) or simple transactional information, such as necessary to process payments.

One solicitation – ITAR – JCP – CDI (DFARS 252.204-7012) & FCI (FAR 52.204-21)

Distribution Statement A - example



Attachment to client email

2/5/2020

Distribution Statements – as an example

- A. Approved for public release.
- B. U.S. Government agencies only
- C. U.S. Government agencies and their contractors
- D. Department of Defense and U.S. DoD contractors only
- E. DoD Components only
- F. Further dissemination only as directed by

DoD Instruction 5230.24 August 23, 2012

Hypothetical – maybe not



Hypothetical with an evil twist – of course

- Scrap/recycling company is new
- Attractive price for new or transitioning customers
- Contract – service agreement signed
- Service initiated
- No due-diligence
- Company does not qualify as a U.S. Person
- Scrap/recycling is a ruse – mining DoD manufacturer's waste stream
- Items select and sold/sent to

CUI = Single State Information – so what?

SPECIAL PUBLICATION 800-171
REVISION 1

PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN
NONFEDERAL SYSTEMS AND ORGANIZATIONS

IMPLEMENTING A SINGLE STATE SECURITY SOLUTION FOR CUI

Controlled Unclassified Information has the *same value*, whether such information is resident in a federal system that is part of a federal agency or a nonfederal system that is part of a nonfederal organization. Accordingly, the security requirements contained in this publication are consistent with and complementary to the standards and guidelines used by federal agencies to protect CUI.

Reference – DD Form 2345 - JCP

NUMBER 5230.25
November 6, 1984

Incorporating Change 1, August 18, 1995
USDR&E

SUBJECT: Withholding of Unclassified Technical Data From Public Disclosure

REFERENCES, continued

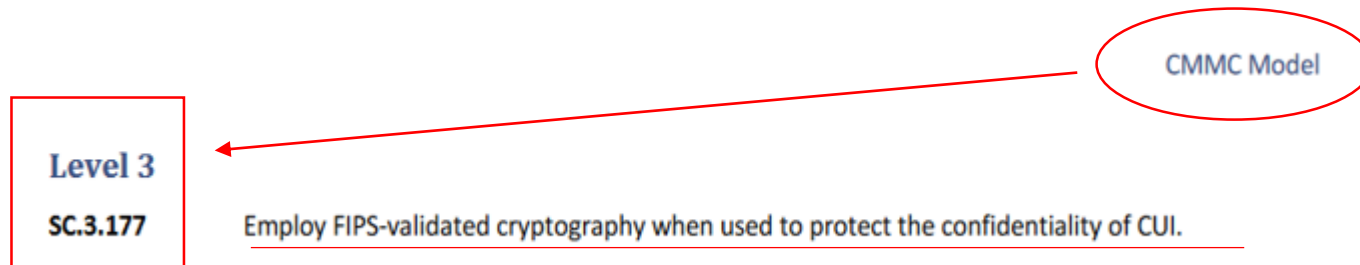
- References: (a) Title 10, United States Code, Section 140c, as added by Public Law 98-94, "Department of Defense Authorization Act, 1984," Section 1217, September 24, 1983
- (b) Executive Order 12470, "Continuation of Export Control Regulations," March 30, 1984
- (c) Public Law 90-629, "Arms Export Control Act," as amended (22 U.S.C. 2751 et seq.)
- (d) through (n), see enclosure 1

- (d) DoD Instruction 5200.21, "Dissemination of DoD Technical Information," September 27, 1979
- (e) DoD 5400.7-R, "DoD Freedom of Information Act Program," December 1980
- (f) Export Administration Regulations
- (g) International Traffic in Arms Regulations
- (h) DoD Federal Acquisition Regulation Supplement
- (i) Public Law 89-487, "Freedom of Information Act," as amended (5 U.S.C. 552(b)(3) and (4))
- (j) Executive Order 12356, "National Security Information," April 2, 1982
- (k) DoD 5200.1-R, "Information Security Program Regulation," August 1982
- (l) DoD Directive 5230.24, "Distribution Statements on Technical Documents," November 20, 1984
- (m) Militarily Critical Technologies List, October 1984
- (n) DoD Instruction 7230.7, "User Charges," June 12, 1979

3.8.1 Protect (i.e., physically control and securely store) system media containing CUI, both **paper and digital**.

NIST (SP) 800-171 Revision 1, December 2016

FIPS - encryption



§120.54 Activities that are not exports, reexports, retransfers, or temporary imports.

(a) The following activities are not exports, reexports, retransfers, or temporary imports:

(5) Sending, taking, or storing technical data that is: (i) Unclassified; (ii) Secured using end-to-end encryption; (iii) Secured using cryptographic modules (hardware or software) compliant with the Federal Information Processing Standards Publication 140–2 (FIPS 140–2) or its successors, supplemented by software implementation, cryptographic key management, and other procedures and controls that are in accordance with guidance provided in current U.S. National Institute for Standards and Technology (NIST) publications, or by other cryptographic means that provide security strength that is at least comparable to the minimum 128 bits of security strength achieved by the Advanced Encryption Standard (AES– 128);

DEPARTMENT OF STATE 22 CFR Part 120 [Public Notice: 10946] RIN 1400–AE76

International Traffic in Arms Regulations: Creation of Definition of Activities That Are Not Exports, Reexports, Retransfers, or Temporary Imports;
Creation of Definition of Access Information; Revisions to Definitions of Export, Reexport, Retransfer, Temporary Import, and Release

Windows and FIPS encryption

FIPS 140-2 standard overview

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products, as defined in Section 5131 of the Information Technology Management Reform Act of 1996.

The [Cryptographic Module Validation Program \(CMVP\)](#), a joint effort of the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS), validates cryptographic modules against the Security Requirements for Cryptographic Modules (part of FIPS 140-2) and related FIPS cryptography standards. The FIPS 140-2 security requirements cover eleven areas related to the design and implementation of a cryptographic module. The NIST Information Technology Laboratory operates a related program that validates the FIPS approved cryptographic algorithms in the module.

<https://docs.microsoft.com/en-us/windows/security/threat-protection/fips-140-validation>; November 4, 2019

Information management considerations

- ITAR – Definition: Defense Article
- This term includes technical data recorded or stored in any physical form, models, mockups or other items that reveal technical data directly relating to items designated in §121.1 of this subchapter. It also includes forgings, castings, and other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable by mechanical properties, material composition, geometry, or function as defense articles.

22 CFR §120.6 Defense article.

Some things

- Mindset
- Commitment
- Resources
- Awareness of programs and their requirements
- References
- Training
- Maintenance & updates

Develop your key questions – such as

- How do you know?
- How do you identify?
- How do you account for?
- How do you track?
- Who can access?
- Do you have processes and procedures?
- What records do you maintain/retain?
- How frequently do you test?

Establish and Maintain a Compliance Program

Program elements:

- Fully supported by senior management
- Regularly reviewed/updated
- Research & apply references
- Clearly documented in writing
- Tailored to the business
- Tailored to information being handled
- Training (periodic/as needed) conducted; documented
- Outward looking component – feedback, current external issues

Create/manage information census

- Identify –
 - Information held
 - Responsible individual
 - Location
 - Program
 - Storage requirements
 - Marking requirements
 - Sharing restrictions
 - Destruction requirements
 - Update records as needed

Key management/security requirements

- Solicitation Review
- Identification of data/information requirements
- Identify team members
- Advise of requirements
- Create limited access space
- Control access, information and time (functional, specified, unlimited)
- Detail requirements – sharing, copying, transmission

Training

Train: Teach individuals the concepts to perform the functions within the organization and how to be an asset. Implement entry-level professional education. Ensure training is relevant and updated to keep pace with the changing environment.

cyber poses to successful mission accomplishment. The annual cybersecurity training, currently required by DoD, is insufficient in providing that training to the overall workforce. It is slow to change and does not sufficiently relate the threat to the individual in ways that are understandable and relevant to their jobs and the missions they are performing. Evaluating training effectiveness by simply clicking through electronic training that is virtually identical to the previous year does not increase user level knowledge or reduce risk.

New Terms to take note of -

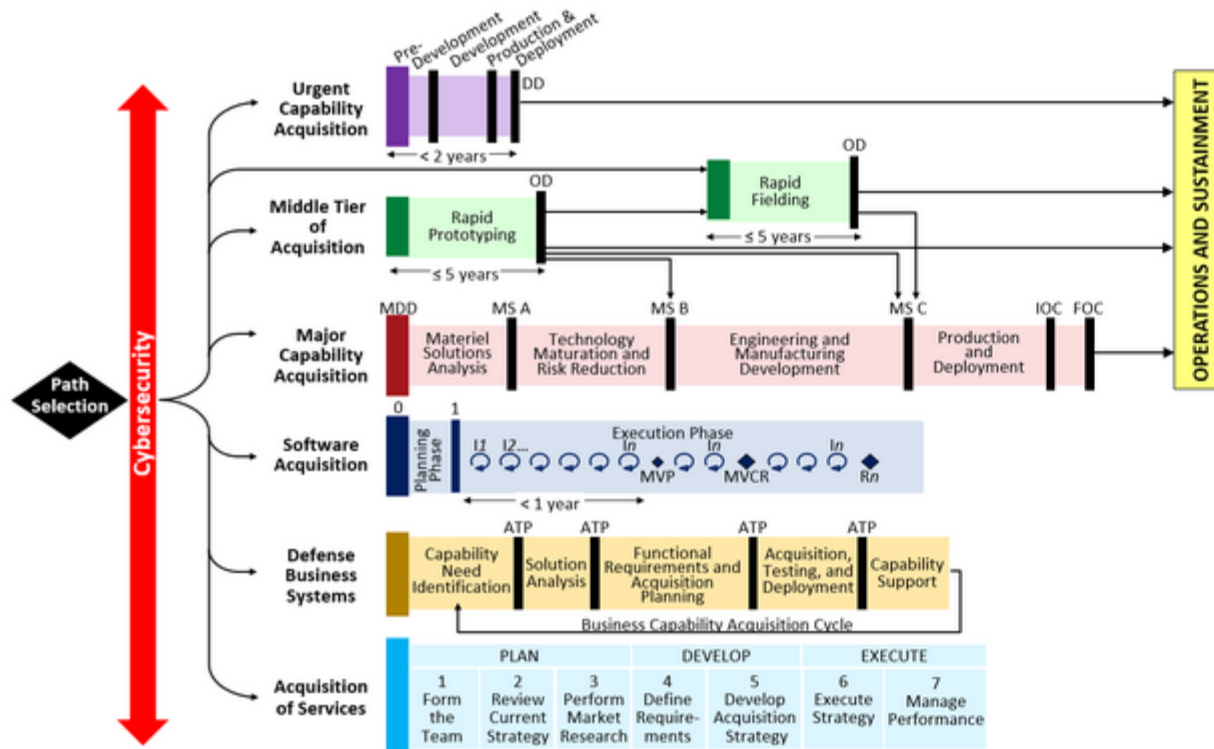
- Adaptive Acquisition Framework – see: <https://aaf.dau.edu>
 - DoD Instruction 5000.02 Effective January 23, 2020
<https://www.esd.whs.mil/DD/>
- Six different Acquisition pathways

[Home](#)[Pathways](#) ▾[Guidance](#) ▾[Policies and Guides](#)[AAF Feedback](#)

“The Adaptive Acquisition Framework will be the most transformational acquisition policy change we’ve seen in decades.”

Ms. Ellen Lord, USD(A&S)

Adaptive Acquisition Framework



A set of acquisition pathways to enable the workforce to tailor strategies to deliver better solutions faster.

Jump to the Pathways

Help Me Select a Pathway

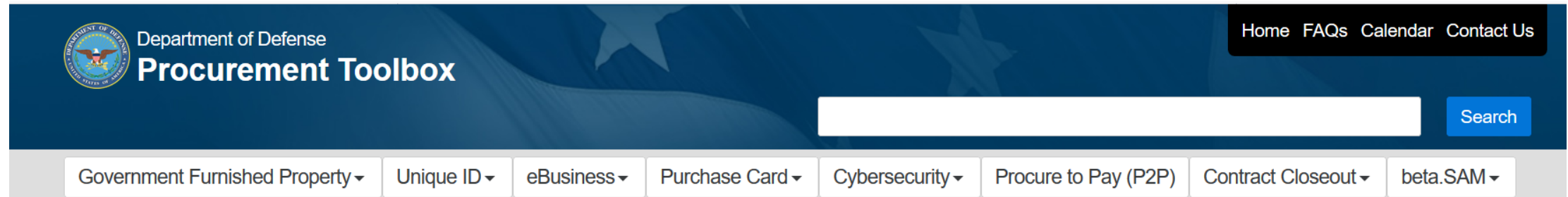
<https://aaf.dau.edu/>

2/5/2020

Useful resources

- CMMC Model v1.0 – <https://www.acq.osd.mil/cmmc> PDF (28 pages)
- CMMC Model v1.0 Appendices PDF (338 pages)
 - References Appendix F - 83
- Jan 31, 2020 Press Briefing video
- Jan 31, 2020 Press Briefing transcript – <https://www.defense.gov>
- CMMC Accreditation Board - <https://www.cmmcab.org>
- CUI – <https://www.archives.gov/cui> > CUI Registry
- CUI Implementing Directive – 32 CFR Part 2002
- Federal Contract Information (FCI) 48 CFR 52.204-21
- DFARS 252.204-7012 – NIST 800-171 r!

DoDProcurementtoolbox.com



The screenshot shows the top navigation bar of the DoD Procurement Toolbox website. On the left is the Department of Defense seal and the text "Department of Defense Procurement Toolbox". On the right is a navigation menu with links for "Home", "FAQs", "Calendar", and "Contact Us". Below the navigation bar is a search bar with a "Search" button. At the bottom of the header is a horizontal menu with dropdown arrows for "Government Furnished Property", "Unique ID", "eBusiness", "Purchase Card", "Cybersecurity", "Procure to Pay (P2P)", "Contract Closeout", and "beta.SAM".

Department of Defense Procurement Toolbox

A collection of tools and services to help you and your organization manage, enable, and share procurement information across the Department of Defense.

<https://dodprocurementtoolbox.com/>

- **Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting**
 - https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html

Additionally, there is an interesting Open DFAR case

| | | | |
|-----------|---|--|---|
| 2019-D041 | Strategic Assessment and Certification Cybersecurity Requirements | Implements a standard DoD-wide methodology for assessing DoD contractor compliance with all security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. | 01/15/2020 DARC agreed to draft proposed DFARS rule. Case manager processing. |
|-----------|---|--|---|

Strategically Implementing Cybersecurity Contract Clauses

Per my direction on February 5, 2019, Strategically Implementing Cybersecurity Contract Clauses (<https://www.acq.osd.mil/dpap/pdi/cyber/index.html>), the Director, Defense Contract Management Agency (DCMA), in partnership with the Acting Principal Director, Defense Pricing and Contracting (DPC), the DoD Chief Information Officer, the Office of the Under Secretary of Defense for Research and Engineering, the Office of the Under Secretary of Defense for Intelligence, and other DoD Components, developed the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment Methodology, Version 1.0 (<https://www.acq.osd.mil/dpap/pdi/cyber/index.html>). This standard methodology enables the strategic assessment of a contractor's implementation of NIST SP 800-171, "Protecting CUI In Nonfederal Systems and Organizations," a requirement for compliance with Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting."

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

■ February 12, 2020

Introduction to Certifications Available to Woman Owned Businesses

[CLICK HERE](#) for additional information

Presented by Shane Mahaffy, U.S. Small Business Administration and Kim Garber, Wisconsin Procurement Institute (WPI)

■ February 12, 2020

Introduction to Certifications Available to Minority Owned Businesses

[CLICK HERE](#) for additional information

Presented by Benjamin Blanc, Wisconsin Procurement Institute (WPI)

■ February 18, 2020

Data Insight for Gov't Contractors – Turning Data Into Usable Information

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

■ February 25, 2020

State and Federal Certifications for Veteran and Service Disabled Veteran Owned Businesses

[CLICK HERE](#) for additional information

Presented by Shane Mahaffy, U.S. Small Business Administration and Mark Dennis, Wisconsin Procurement Institute (WPI)

ACQUISITION HOUR LIVE WEBINARS SERIES

▪ February 26, 2020

Learning About the Surety Bond Guarantee From the U.S. SBA

[CLICK HERE](#) for additional information

Presented by Tamara Murray, U.S. Small Business Administration

▪ March 17, 2020

Market Segmentation for Enhanced Business Development

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

▪ March 4, 2020

Basics of the Federal Procurement Data Systems (FPDS)

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

▪ March 18, 2020

Creating Advanced Queries with the Federal Procurement Data System (FPDS)

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

SELLING TO THE US DEPARTMENT OF VETERANS AFFAIRS (VA)

February 11 @ 8:30 am - 11:00 am



Details

Date:

February 11

Time:

8:30 am - 11:00 am

Event Categories:

Workshop, WPI Events

Organizer

Hilary DeBlois

Phone:

(414) 688-3882

Email:

hilaryd@wispro.org

Additional Information

Presented By

Technology Innovation Center (TIC)

US Department of Veterans Affairs (VA)

US Small Business Administration (SBA)

Wisconsin Procurement Institute (WPI)

Event Registration

[Register for Event](#)

Doing contract work for the VA can be challenging. Join WPI to hear about how the VA works, how to respond to solicitations, VA verification process for veteran owned businesses, and maximize your success in selling to the VA. WPI special guest speakers are Steven Maier, VA Small Business Specialist, along with James Strube and Tammie Clendenning from the US Small Business Administration. Small businesses interested in selling to the VA will not want to miss this unique opportunity.

14TH ANNUAL WISCONSIN GOVERNMENT BUSINESS OPPORTUNITIES CONFERENCE (GOBC)

June 24 - June 25

Details

Start:
June 24

End:
June 25

Event Categories:
Conference, WPI Events

Organizer

Hilary DeBlois

Phone:
(414) 688-3882

Email:
hilaryd@wispro.org

Save the Date for the 14th Annual Wisconsin Government Business Opportunities Conference (GOBC) in partnership with Volk Field ANG and Fort McCoy, June 24 and 25th, 2020.

Venue

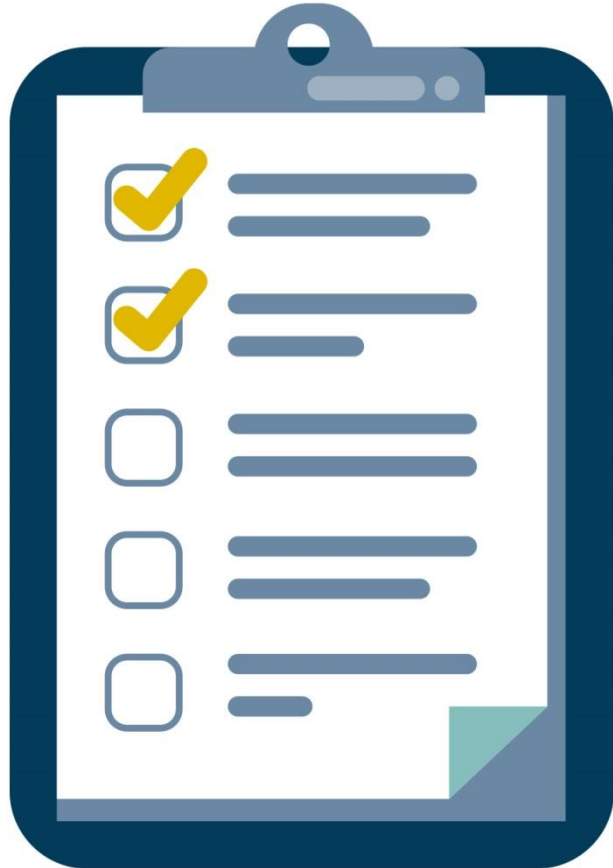
Volk Field Air National Guard Base
100 Independence Drive, Building 475
Camp Douglas, WI 54618 United States + [Google Map](#)



QUESTIONS?



SURVEY



CONTINUING PROFESSIONAL EDUCATION



CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Marc Violante, Wisconsin Procurement Institute

marcv@wispro.org | 920-456-9990

Benjamin Blanc, CFCM, CPPS - Government Contract Specialist

benjaminb@wispro.org | 414-270-3600

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226