Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

HOW THE CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) WILL IMPACT YOUR BUSINESS

ACQUISITION HOUR WEBINAR

April 24, 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!

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.

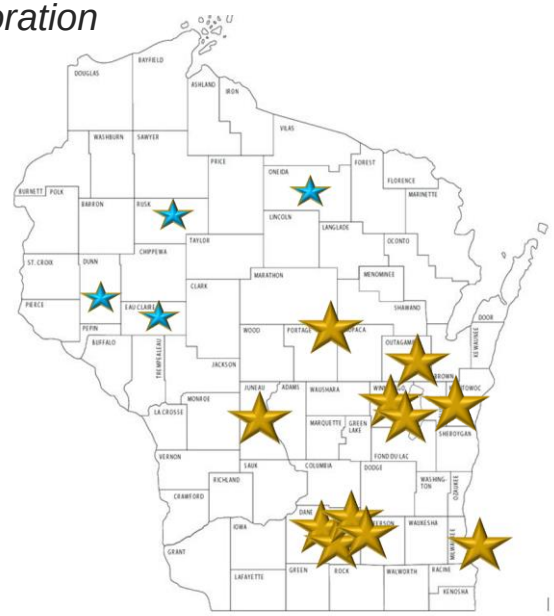
- **INDIVIDUAL CONSELING – At our offices, at clients facility or via telephone/GoToMeeting**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

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

WPI 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*
- **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*



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


Search ...
BLOG
SERVICES
ABOUT
CLIENT PORTAL
SPONSORSHIP
CONTACT
Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)
EVENT CALENDAR
FEDERAL GOVERNMENT
STATE & LOCAL GOVERNMENT
GRANTS
SUCCESS & AWARDS
FAQS
CURRENT EDITION OF THE WPI NEWSLETTER
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)
www.wispro.org
GET STARTED WITH THE BASICS
Questions & answers on how to get started.
SIGN-UP FOR OUR NEWSLETTER
Stay up-to-date with the latest WPI news.
HAVE A QUESTION? WE'RE HERE TO HELP.
One of our staff of experts is available to answer your questions.

CMMC

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

Marc N. Violante

Wisconsin Procurement Institute

April 24, 2020

What we know - Current Cyber Obligations

- 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems
- 252.204-7008 - Compliance with safeguarding covered defense information controls
- 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting
- DON – Geurts memos – CDRL requirements
- Other requirements

Information Security Obligations/Requirements

- 252.204-7000 – Disclosure of Information
- DOD Directive 5230.25 Withholding of Unclassified Technical Data from Public Disclosure
- DOD Instruction 5230.24 Distribution Statements on Technical Documents
- Canadian Technical Data Control Regulations (TCDR)
- State Department, Directorate of Defense Trade Controls
- Commerce Control List
- DLA Requirements –
  - DLA Export Control Data Access

What we don't know

- New DFARs (Strategic Assessment) – in addition to 252.204-7012
- Definitions of/examples of products/services contained in each level
- Examples of good-acceptable policies/procedures
- Certification process – "is there more than one correct answer?"
- Timing
  - Inclusion in RFQs/RFPs
  - Specified CMMC v1.x?
  - Assessor process, engagement, scheduling, cost
  - CMMC Level repository, access to and/or use
- Clarity with respect to trainers/consultants/etc
  - "Oklahoma Land Rush" – caveat emptor

CMMC – How much information to expect?

- Some thoughts
  - CMMC v1.2 is published
  - DFARS 252.204-7012 is current
  - DFARS "Strategic Assessment" – draft rule yet to be published
  - CMMC (Level – 1:5) – award determination
  - Procurement information can be CUI - https://www.archives.gov/cui/registry/category-detail/procurement-acquisition.html
    - **Banner Format:** CUI//Category Marking//Limited Dissemination Control
      - Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.
    - **Banner Format:** CUI//Category Marking//Limited Dissemination Control
      - Per FAR 2.101: any of the following information that is prepared for use by an agency for the purpose of evaluating a bid or proposal to enter into an agency procurement contract, if that information has not been previously made available to the public or disclosed publicly: (Items 1-10).

CMMC – it's about the "it's"

- It's not static – it will evolve
- It's not a one size fits all –
  - Different companies,
  - Different requirements
  - Level of complexity
  - Programs need to be
    - Tailored
    - Monitored – evaluated
    - Updated - refreshed
- It's not a checklist – Critical Thinking dominant theme

Topics to consider

- Tunnel vision –
  - Singular focus on CMMC (lack of integration with other requirements)
- Lack of investment
  - time | training | other resources | situational awareness – what's changing?
- Mindset
  - What's important
- Certification via delegation (designation)
  - Lack of active involvement by top management

What are the main issues (barriers)

- Familiarity –What if the question (perspective) were changed?
- Understanding of –
  - Technology
  - Terms
  - Threat
  - How/why process and/or procedures work
    - How does a process solve a problem?
    - Why is documentation needed?
      - How much is enough?
      - What am I trying to show (demonstrate)?
- Why can’t I just say – we are doing that?

The desired end state

- build
  - a cyber-safe,
  - cyber-secure and
  - cyber-resilient

} defense industrial base

Another idea that has been frequently used has been the concept of Critical Thinking

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

CMMC (FCI v. CUI) – important details

Federal Contract Information (FCI)

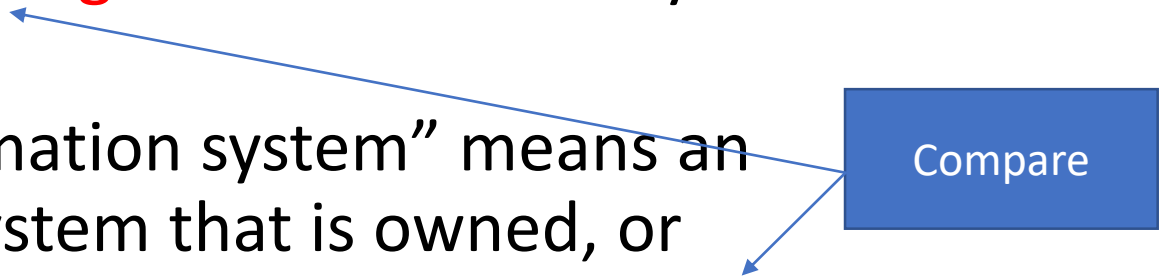
- FAR 52.204-21
  - 15 FAR elements map to 17 CMMC elements
  - Flowdown – substance of clause
- CMMC v1.2

Controlled Unclassified Information (CUI)

- DFARS 252.204-7012
  - Adequate Security (NIST 800-171 r2)
  - Malware ID | Capture | "defang" |share
  - Monitor for incidents
  - Report generation –
    - Medium Assurance Certificate
    - Forensics – freeze 90 days
  - "Include this clause, including this paragraph (m)"
  - CMMC v1.2 – NIST 800-171 r2 + rev b

Apply definitions – track source dates

- the subcontractor may have Federal contract information residing in or transiting through its information system.
  - FAR 52.204-21
- "Covered contractor information system" means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
  - DFARS 252.204-7012
  - SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (DEC 2019)
  - CDI = CTI + CUI



Background – maturity model

- In general, a maturity model is a set of
  - characteristics,
  - attributes,
  - indicators,
  - or patterns
    - that represent capability and progression in a particular discipline.
- provides a benchmark against which an organization can evaluate the current level of capability of its
  - processes, practices, and methods and set goals and priorities for improvement.

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf pg 4

CMMC – definition of a policy

A policy is a high-level statement from an organization's senior management that documents the requirements for a given activity. It is intended to establish organizational expectations for planning and performing the activity, and communicate those expectations to the organization. Senior management should sign policies to show its support of the activity.

At a minimum, the policy should:

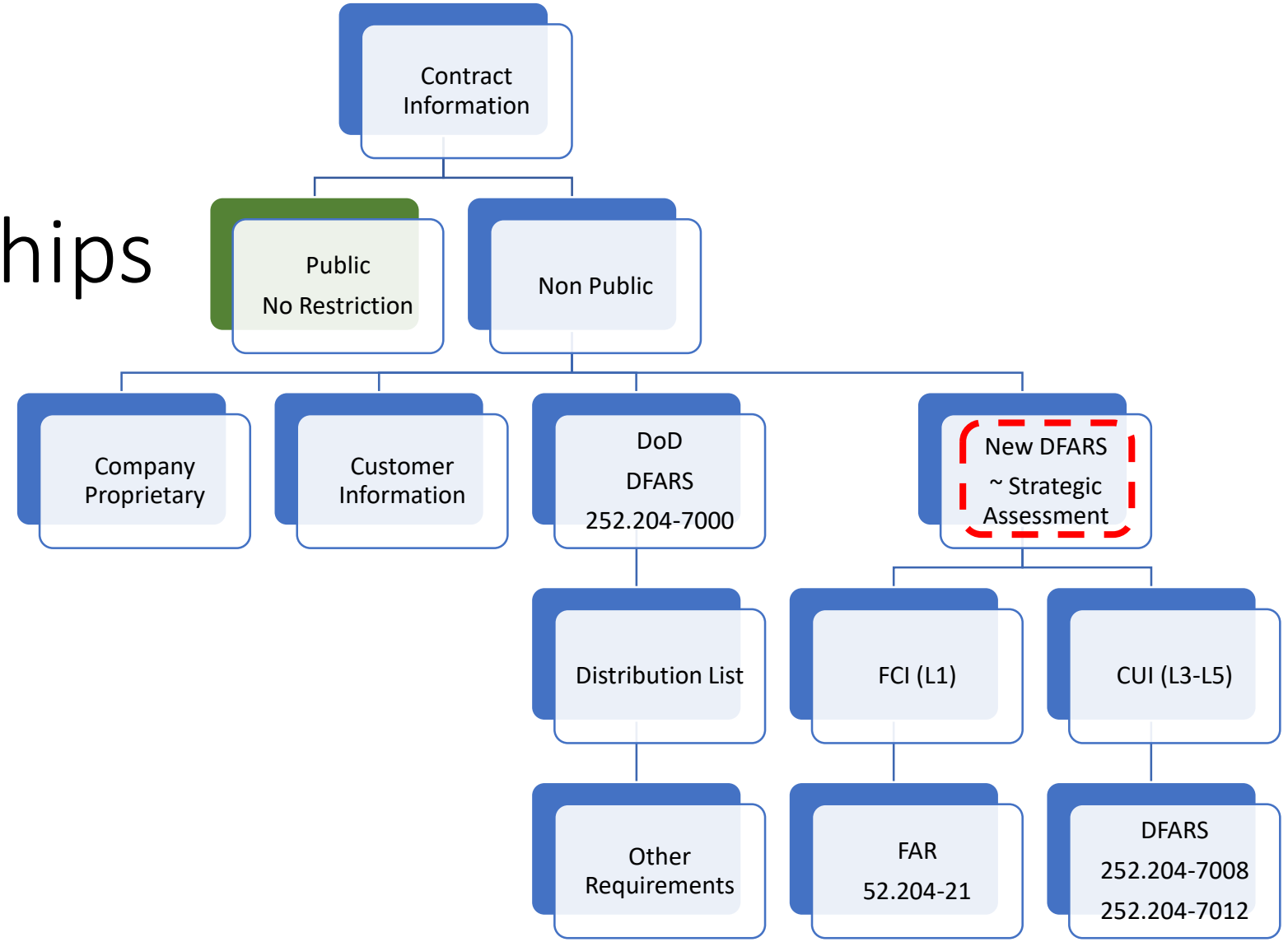
- clearly state the purpose of the policy;
- clearly define the scope of the policy: for example, enterprise-wide, department-wide, or information-system specific;
- describe the roles and responsibilities of the activities covered by this policy: the responsibility, authority, and ownership of [DOMAIN NAME] domain activities; and
- establish or direct the establishment of procedures to carry out and meet the intent of the policy, include any regulatory guidelines this policy addresses.

REFERENCES

- CERT RMM v1.2 GG2.GP1 Subpractice 2

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf B-2

General Relationships



New DFARS

Open DFARS Cases as of April 03, 2020

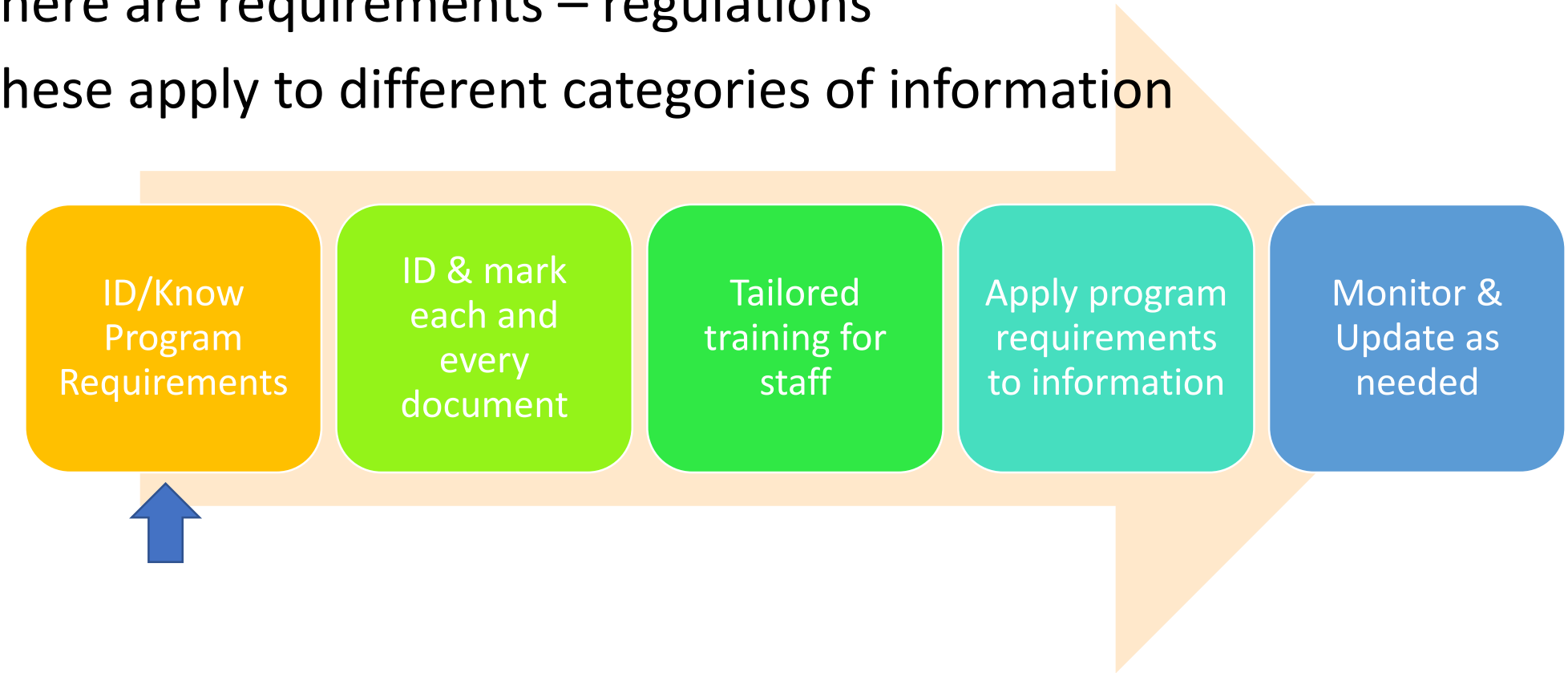
Case Number	Part Number	Title	Synopsis	Status
2019-D041		Strategic Assessment and Cybersecurity Certification Requirements	Implements a standard DoD-wide methodology for assessing DoD contractor compliance with all security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations and a DoD certification process, known as the Cybersecurity Maturity Model Certification (CMMC), that measures a company's maturity and institutionalization of cybersecurity practices and processes. Partially implements section 1648 of the FY20 NDAA.	01/15/2020 DARC agreed to draft proposed DFARS rule. Case manager processing.

Information Security - today

- Categories of information –
  - Federal Contract Information
  - Covered Defense Information = CTI & CUI
  - Controlled Unclassified Information
  - Impact Level
  - Export Controlled
    - JCP
    - ITAR
    - Other
  - Corporate – internal
  - Customer – contract/proprietary

Commonalities

- There are requirements – regulations
- These apply to different categories of information



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

Slight Change

Become familiar with references

Specifications for Minimum Security Requirements

Access Control (AC): Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems; pg 2

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

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 2 – bridge from Level 1 to Level 3 (solicitation will not be Id'd as Level 2)
  - Level 3 – CUI
  - Levels 4 and 5 – small number of companies dealing with highly sensitive CUI
- Periodic recertifications will be required

CMMC – “all companies will be certified

19 - My organization does not handle Controlled Unclassified Information (CUI). Do I have to be certified anyway? –

If a DIB company does not possess CUI but possesses Federal Contract Information (FCI), it is required to meet FAR Clause 52.204-21 and must be certified at a minimum of CMMC Level 1.

Companies that solely produce Commercial-Off-The-Shelf (COTS) products do not require a CMMC certification.

20 - I am a subcontractor on a DoD contract. Does my organization need to be certified? –

Yes, so long as your company does not solely produce COTS products, it will need to obtain a CMMC certificate. The level of the CMMC certificate is dependent upon the type and nature of information flowed down from your prime contractor.

Arrington said at an event Friday the Pentagon will clarify which parts of a contract will demand different levels of certification in upcoming requests for information.
“One size doesn’t fit all for security,” Arrington said. “The subs, by what work they are doing, will need to meet a level one or level two.”

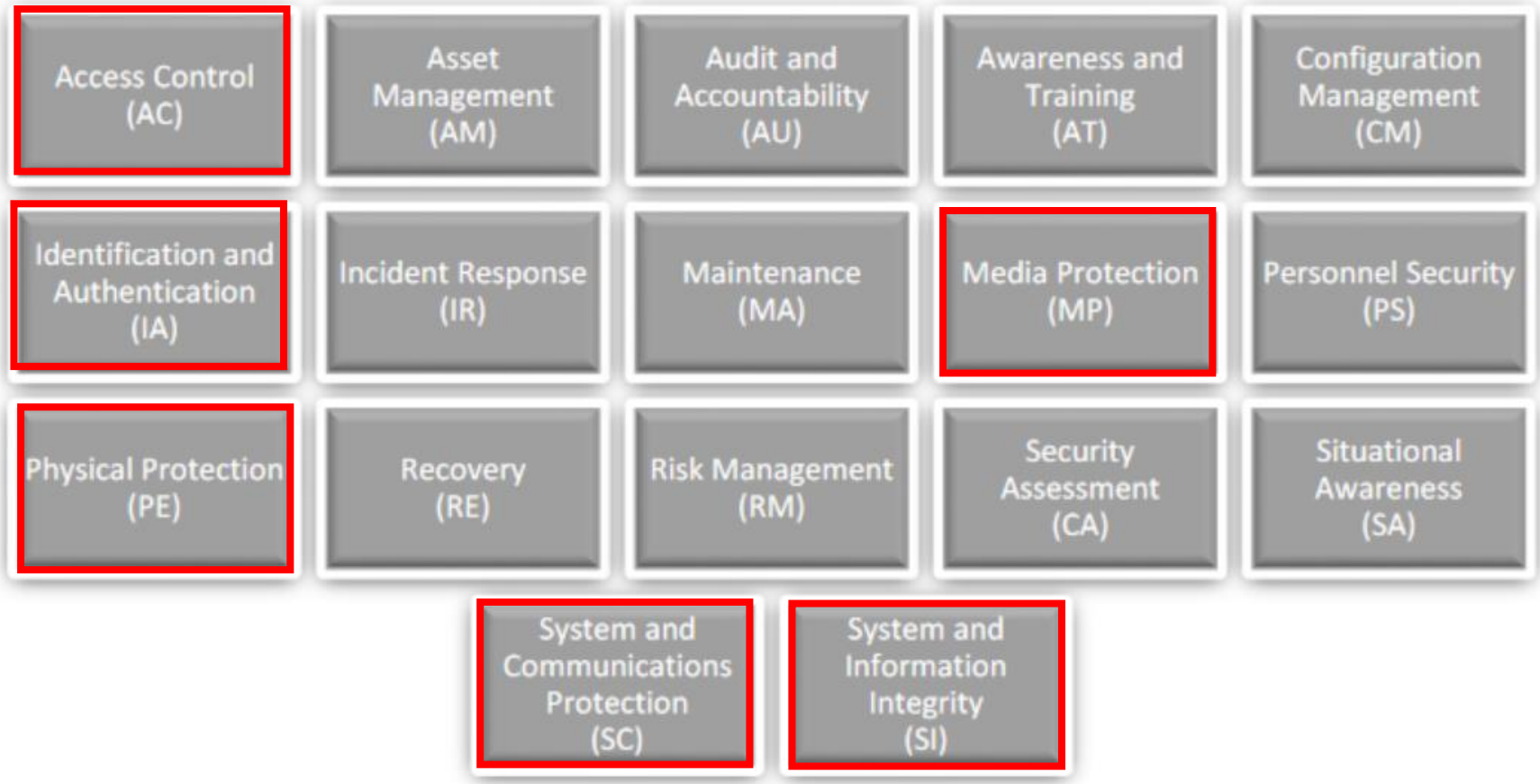
https://www.govconwire.com/2020/03/katie-arrington-firms-wont-need-to-meet-same-level-of-cmmc-requirements-on-contracts/

CMMC – “all companies will be certified

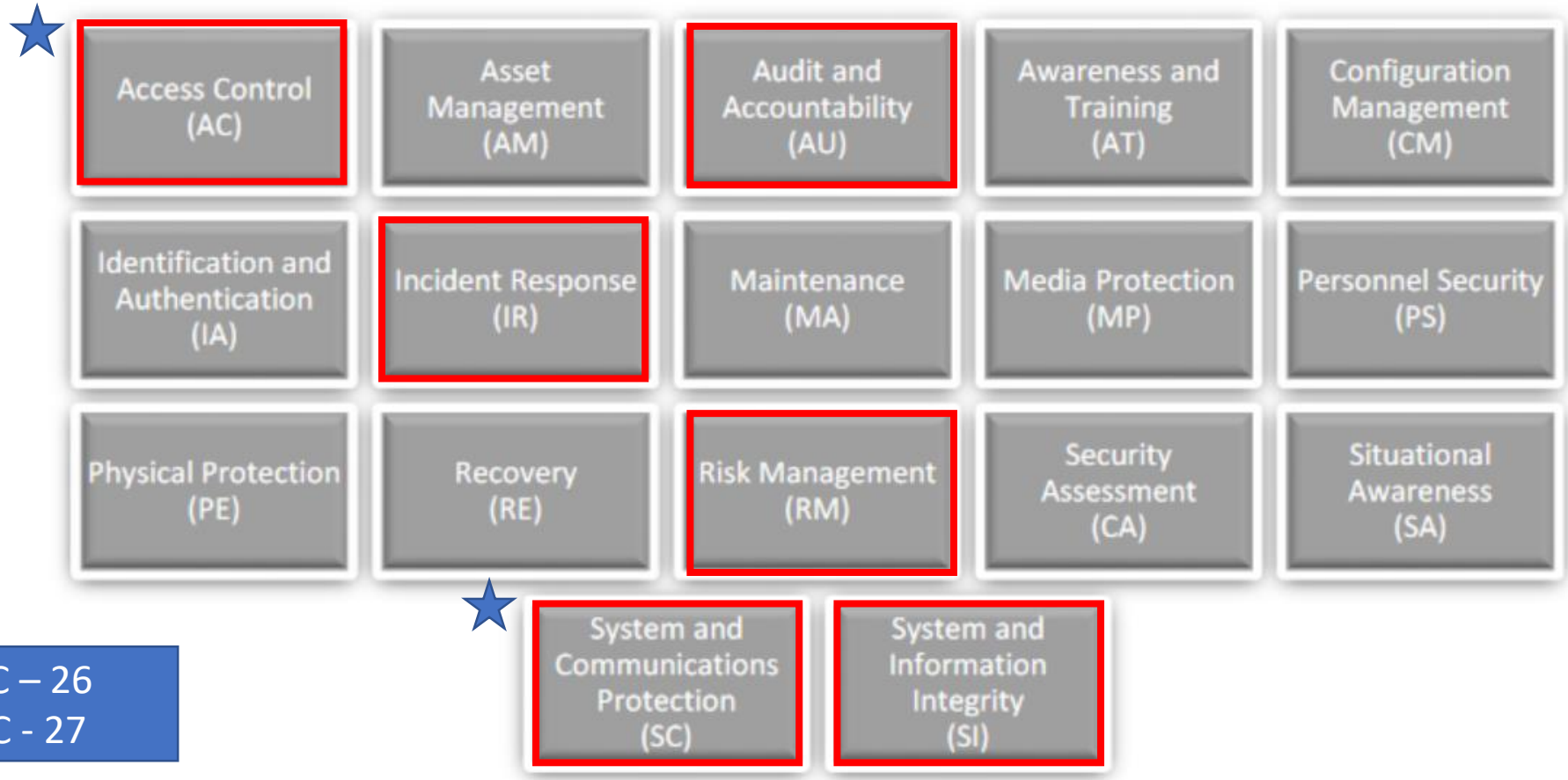
- Assessors will receive a license at a level that matches the assessments they are permitted to conduct. In the very near future, all contractors that do business with the DoD will need to meet at least Level 1 CMMC requirements.

https://www.cmmcab.org/assessors

Figure 4 – CMMC Domains (Red = Level 1)



The “Big Six” (105 of 171 practices)



AC – 26
SC - 27

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf pg 11

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
- Note CMMC v1.0 is being updated and will be replaced by v1.02
- See: https://www.acq.osd.mil/cmmc/updates.html

CMMC A.B.– key players

- CMMC Accreditation Board – see: https://www.cmmcab.org
- Board –
- 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

Board Directory

- Ty Schieber, Board Chairman

- Akin Akinbosoye
- Mark Berman
- Wayne Boline
- Jeff Dalton
- Nicole Dean
- Regan Edens
- James ("Jim") Goepel
- Chris Golden
- Karlton D. Johnson
- Dr. Richard H. 'Doc' Klodnicki
- Valecia Maclin
- Dr. Tim Rudolph
- Ben Tchoubineh
- John Weiler

Under Secretary of Defense Ellen Lord statement on misleading cybersecurity certification information

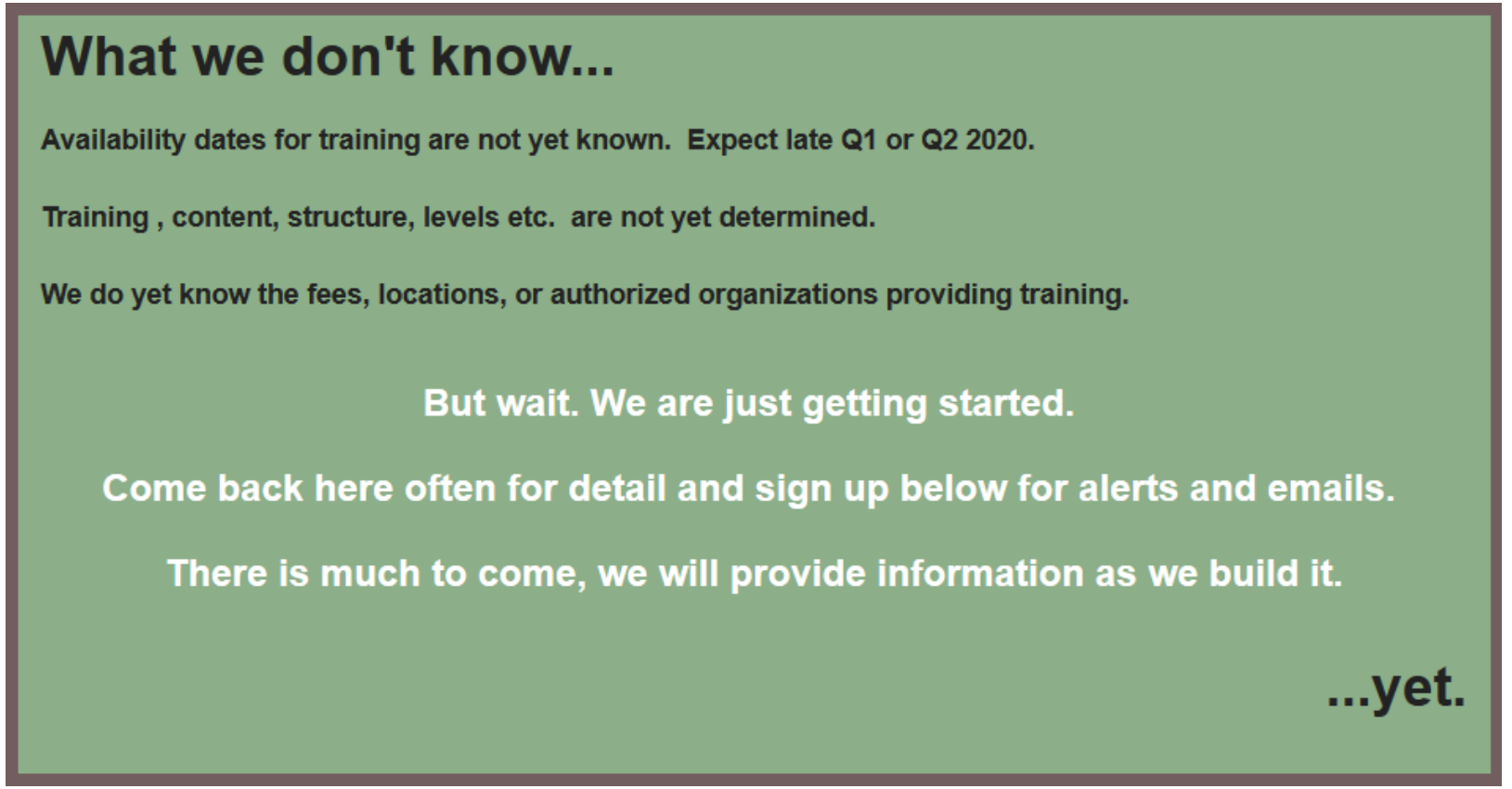
Statement from Under Secretary of Defense Ellen Lord:

- Since I introduced the Cybersecurity Maturity Model Certification model last year, I have consistently stressed the importance of communicating and engaging extensively with industry, academia, military services, the Hill and the public to hear their concerns and suggestions. The purpose of this communication was, and still is, to ensure everyone fully understands the intent, process and requirements of CMMC to fight the very real threats that drive us to require rigorous cybersecurity.

  Unfortunately, the Department has learned that some third-party entities have made public representations of being able to provide CMMC certifications to enable contracting with DoD. The requirements for becoming a CMMC third-party assessment organization (C3PAO) have not yet been finalized, so it is disappointing that some are trying to mislead our valued business partners. To be clear, there are no third-party entities at this time who are capable of providing a CMMC certification that will be accepted by the Department. At this time, only training materials or presentations provided by the Department will reflect our official position with respect to the CMMC program. I have also reached out to the presidents of the PSC, AIA and NDIA industry associations to make them aware as well, and they remain connected with my CMMC team.

https://www.cmmcab.org/

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



Note: **Assessors are required to obtain a security clearance. The specific clearance levels are not yet determined.**

https://www.cmmcab.org/assessors

Prospective Assessors & C3PAOs

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.

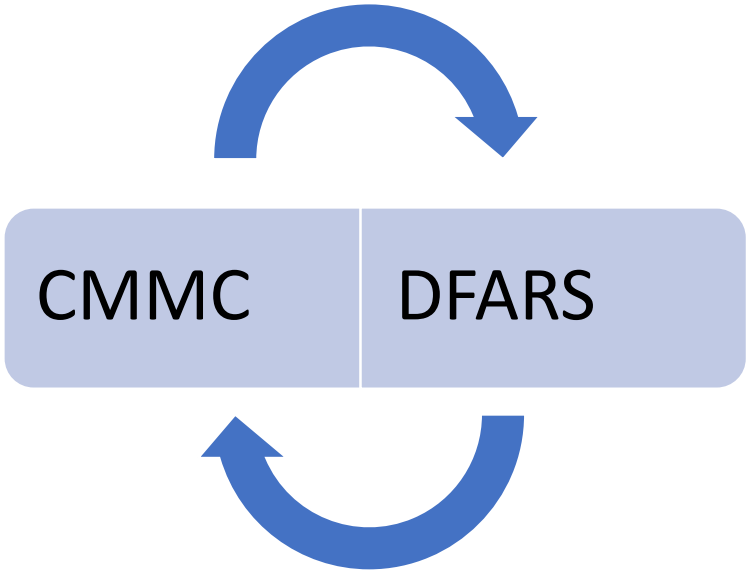
What about pre-assessments?

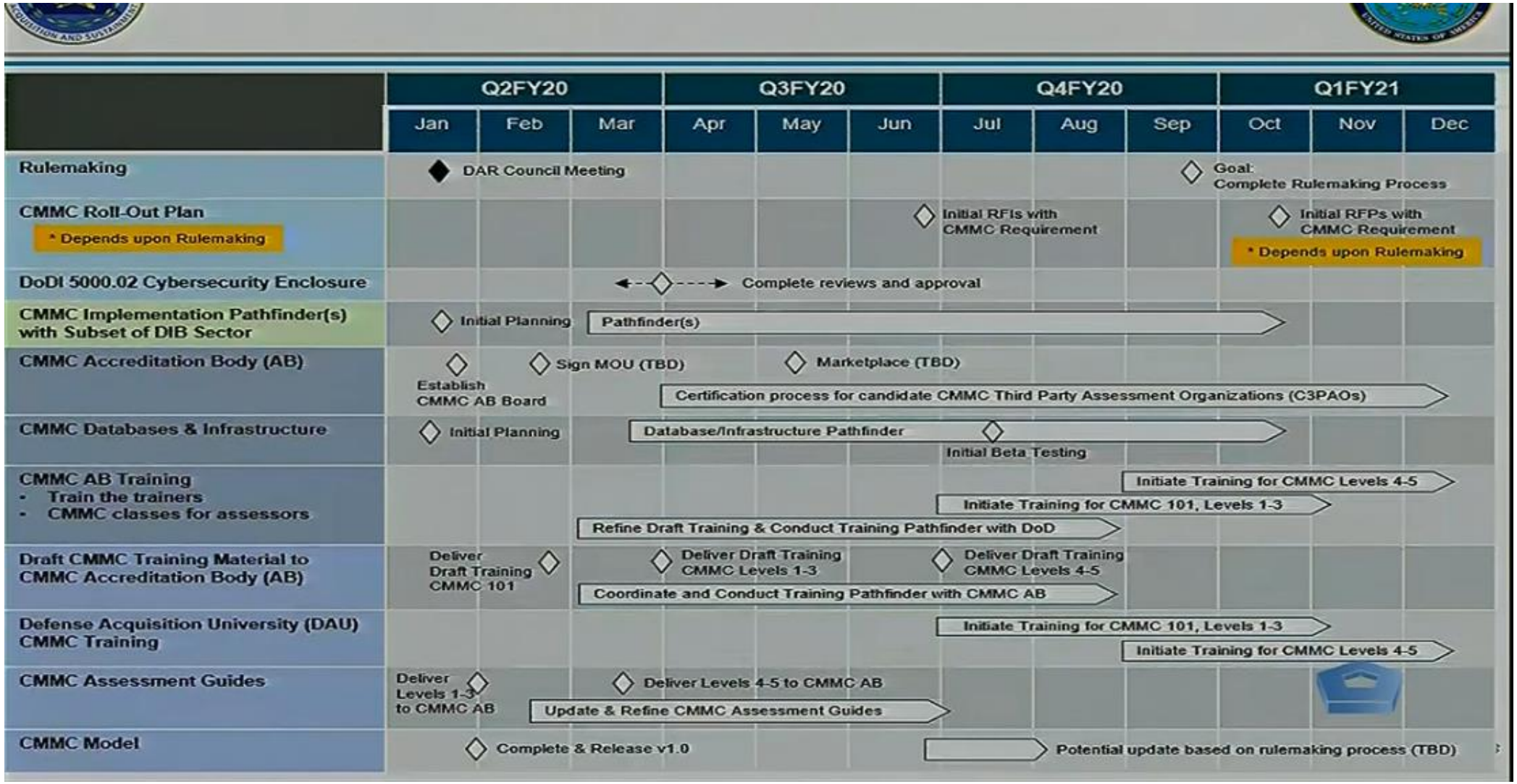
- To be clear, offering pre-assessments or consulting using the most current draft of the standard is acceptable and encouraged. However, it is not currently appropriate for any vendor to offer a formal CMMC assessment claiming that is authorized by the CMMC-AB.

https://www.cmmcab.org/faq

Time Line

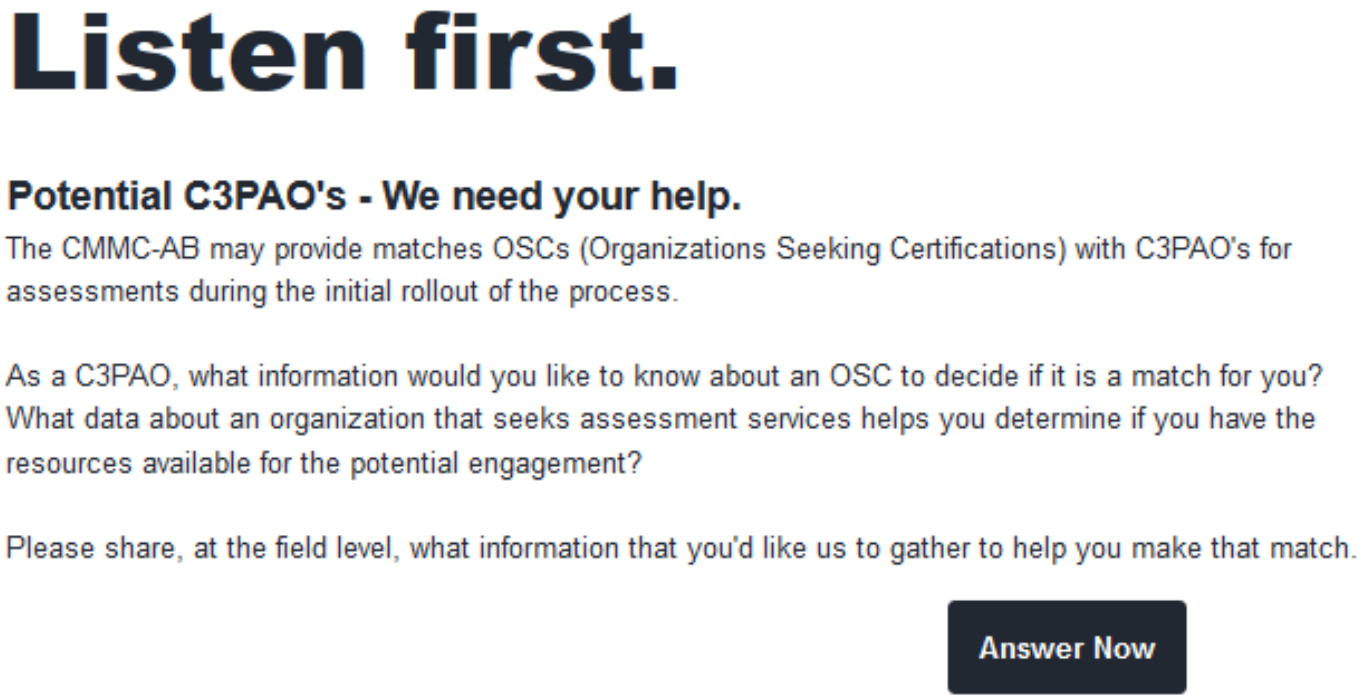
- Late spring/early summer timeframe to complete a new defense acquisition regulation, a new Defense Federal Acquisition Regulation, or DFAR.
- CMMC requirement in selected RFIs [request for information] in the June 2020 timeframe
- Corresponding RFPs [request for proposals] in September 2020 time frame,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





Timeline charge from January 31, 2020 Press Briefing

Active Development Process



https://www.cmmcab.org/ scroll to bottom of home page

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.

Ms Arrington, Press Briefing transcript, January 31, 2020

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.

CMMC Marketplace – new information

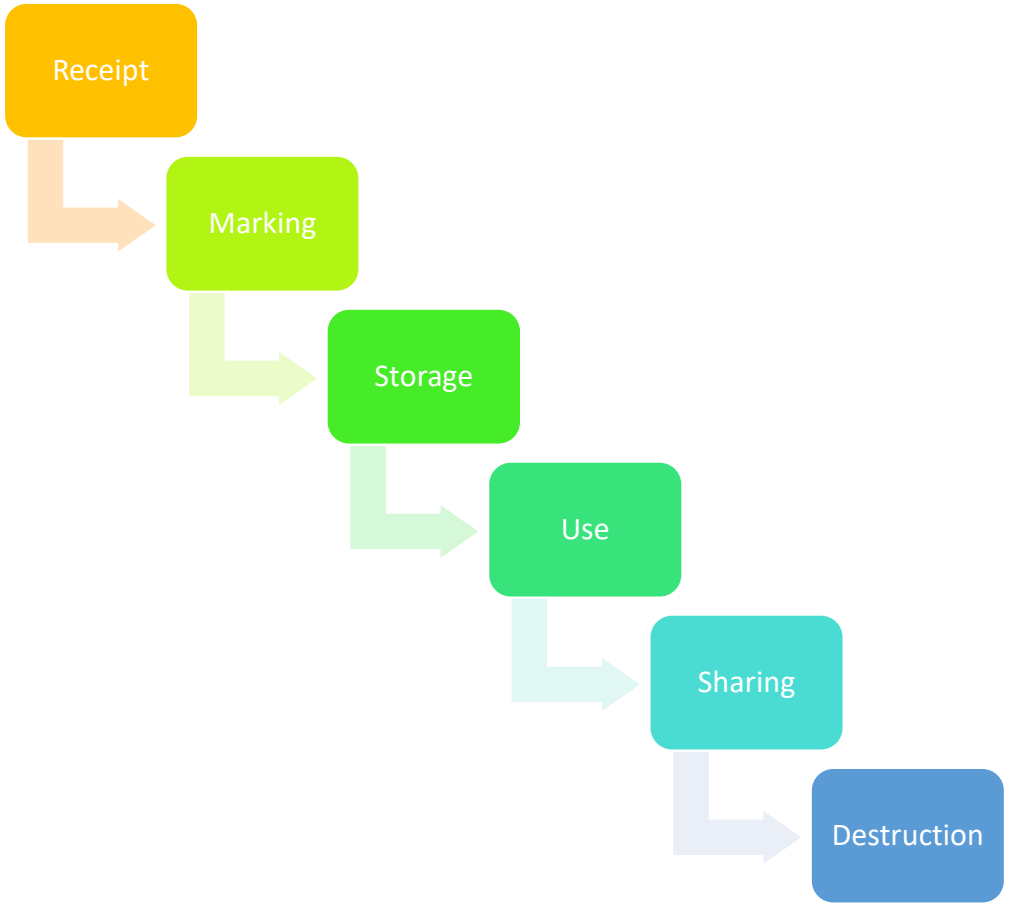
- MOU (DoD & CMMC-AB has been signed)
- DFARS case in progress; new rule by end of FY
- First training class in progress
- Possible COVID related delays
- Pathfinder contracts initiated
- Initial CMMC activity with Missile Command
- At completion of ___ six month ramp up to full implementation
- Questions concerning certification of all subcontractors
- Be watchful of “posers”; those offering certification. There are none!

Related to "Critical Thinking" and integration of various requirements

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

M.N. Violante, WPI – Nov 2017

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

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

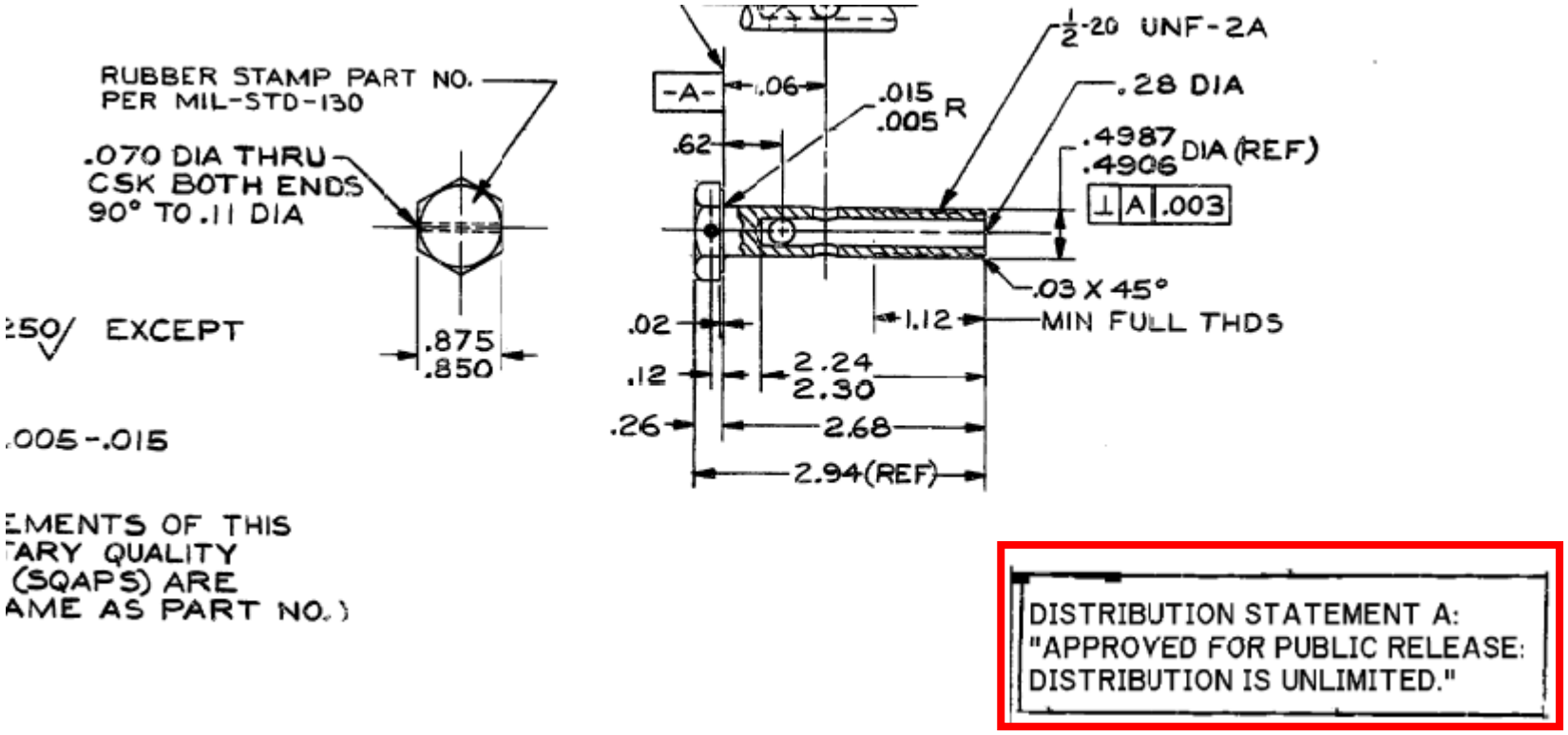
(a) Definitions. As used in this clause-

"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

Distribution Statement A – example 2

Cybersecurity Maturity Model Certification (CMMC)

CMMC Model v1.0

31 January 2020

DISTRIBUTION A. Approved for public release

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 controlling office

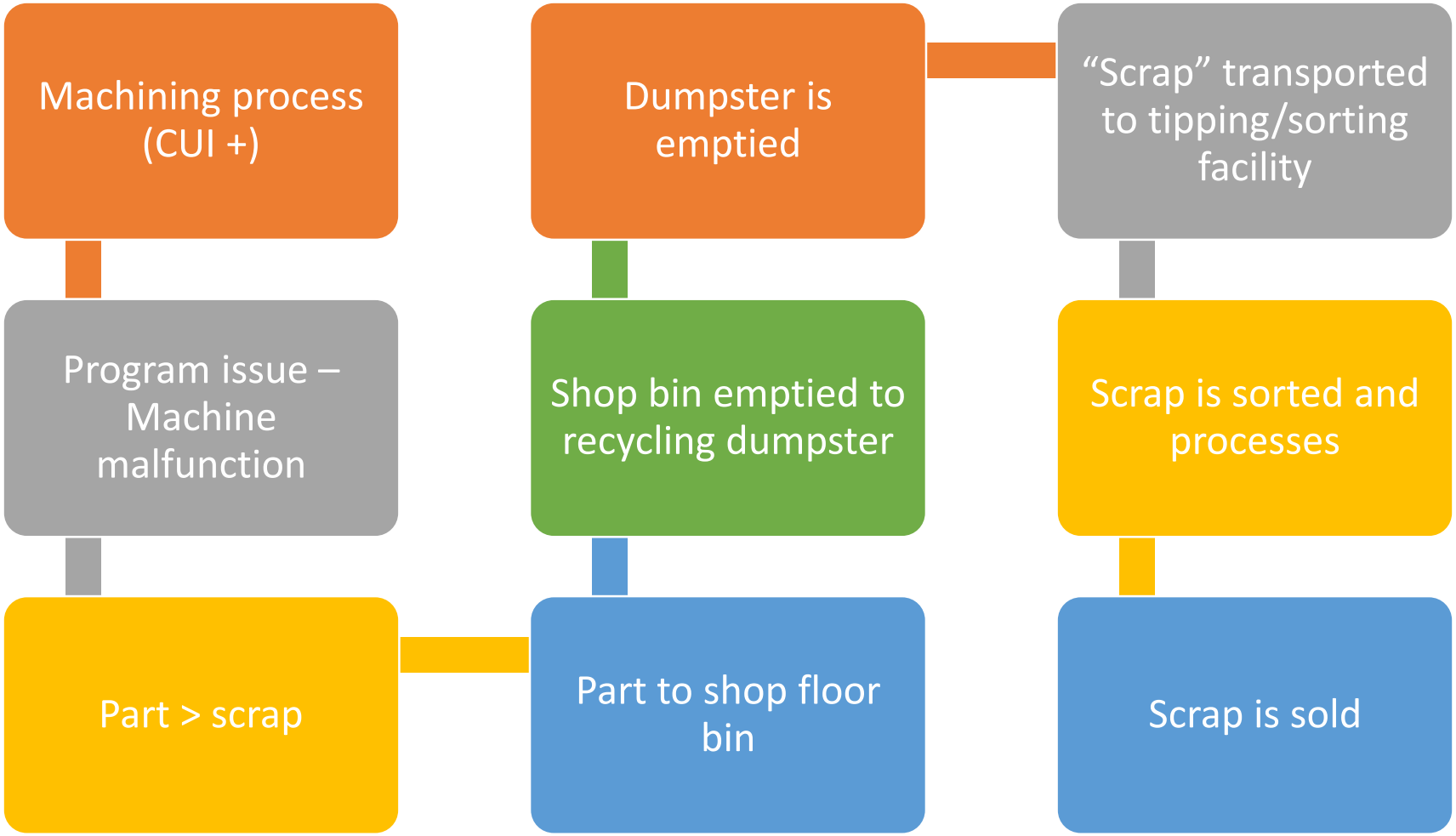
DoDI 5230.24, August 23, 2012 Change 3, 10/15/2018

THIRD PARTY-IMPOSED DISTRIBUTION STATEMENTS

- Contractors are generally allowed to retain ownership of the intellectual property that is embodied in technical data, documents, or information that is delivered or otherwise provided to the Government.
- Restrictive markings are either required or permitted on all forms of technical data or computer software that is to be delivered to DoD.

DoDI 5230.24, August 23, 2012 Change 3, 10/15/2018

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 ….

Checklist – No – First Principles - Yes

Do not allow sensitive information, including Federal Contract Information (FCI), which may include CUI, to become public. It is important to know which users/employees are allowed to publish information on publicly accessible systems, like your company website. Limit and control information that is posted on your company's website(s) that can be accessed by the public.

Example

You are head of marketing for your company and want to become better known by your customers. So, you decide to start issuing press releases about your company projects. Your company gets FCI from doing work for the Federal government. FCI is information that is not shared publicly. Because you recognize the need to control sensitive information, including FCI, you carefully review all information before posting it on the company website or releasing to the public. You allow only certain employees to post to the website.

REFERENCES

- FAR Clause 52.204-21 b.1.iv
- NIST SP 800-171 Rev 1 3.1.22
- NIST SP 800-53 Rev 4 AC-22

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf B-14

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.

NIST SP 800-171 r1, page 6

Reference – DD Form 2345 - JCP

NUMBER 5230.25
November 6, 1984

Incorporating Change 2, October 15, 2018
USD(R&E)

SUBJECT: Withholding of Unclassified Technical Data From Public Disclosure

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 (o), see enclosure 1

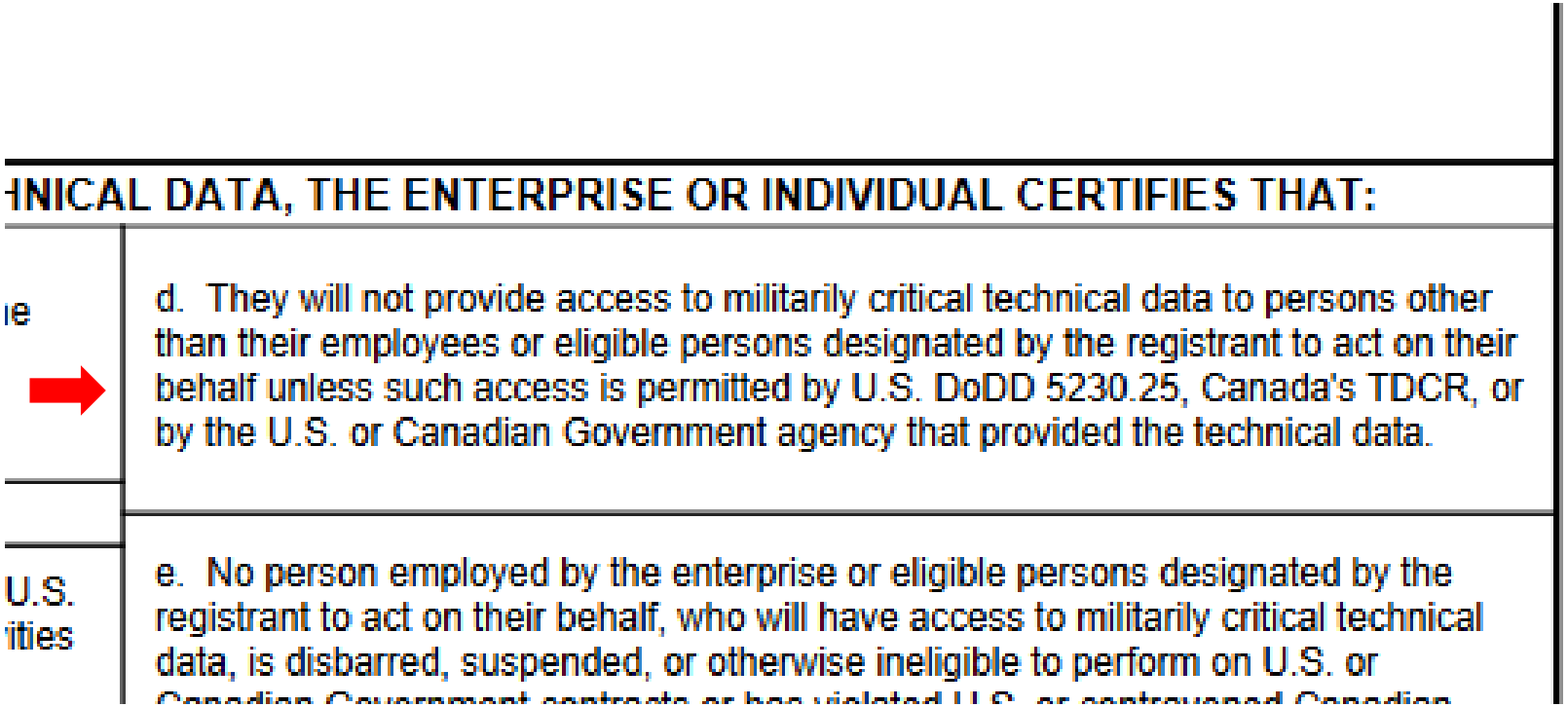
REFERENCES, continued

(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

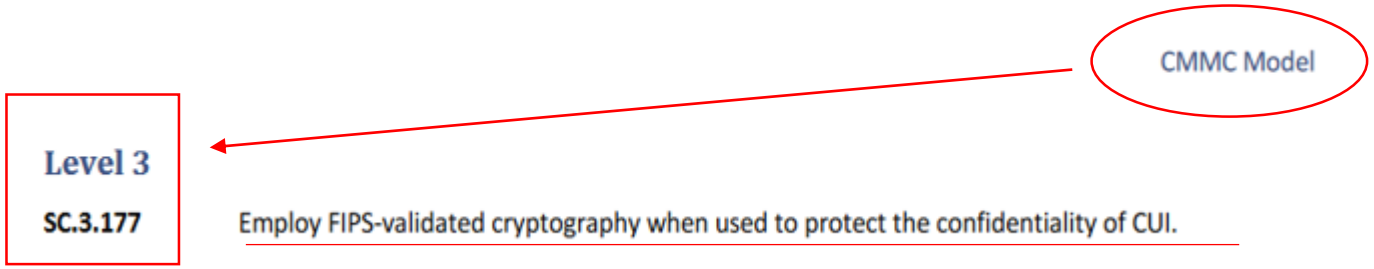
Identify relationships and references



HNICAL DATA, THE ENTERPRISE OR INDIVIDUAL CERTIFIES THAT:

ıe	d. They will not provide access to militarily critical technical data to persons other than their employees or eligible persons designated by the registrant to act on their behalf unless such access is permitted by U.S. DoDD 5230.25, Canada's TDCR, or by the U.S. or Canadian Government agency that provided the technical data.
U.S. ities	e. No person employed by the enterprise or eligible persons designated by the registrant to act on their behalf, who will have access to militarily critical technical data, is disbarred, suspended, or otherwise ineligible to perform on U.S. or

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 you 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.

Secretary of the Navy, Cybersecurity Readiness Review, March 2019, page s 19 &20

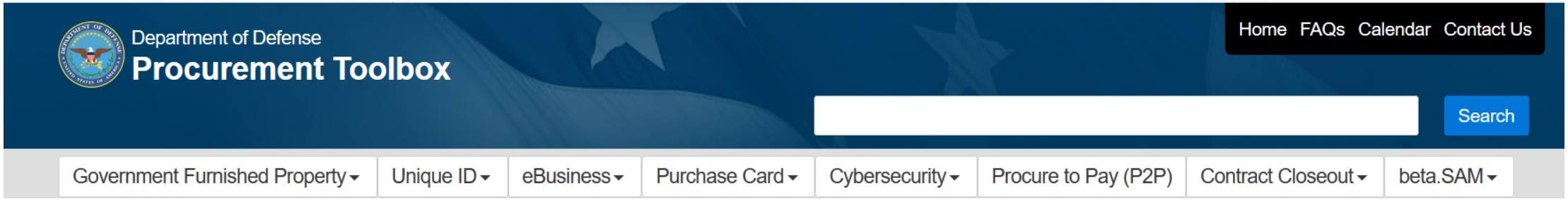
Useful resources

- 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 r1

News Worthy

- **NIST SP 800-53 Revision 5 Represents a Multi-Year Effort to Develop Next-Generation Security and Privacy Controls**
  - The National Institute for Standards and Technology (NIST) has published the draft version of **SP 800-53 (revision 5)**: Security and Privacy Controls for Information Systems and Organizations. This is the first update to SP 800-53 since revision 4 was published seven years ago, and reflects the major changes to the security landscape over the last few years.

DoDProcurementtoolbox.com

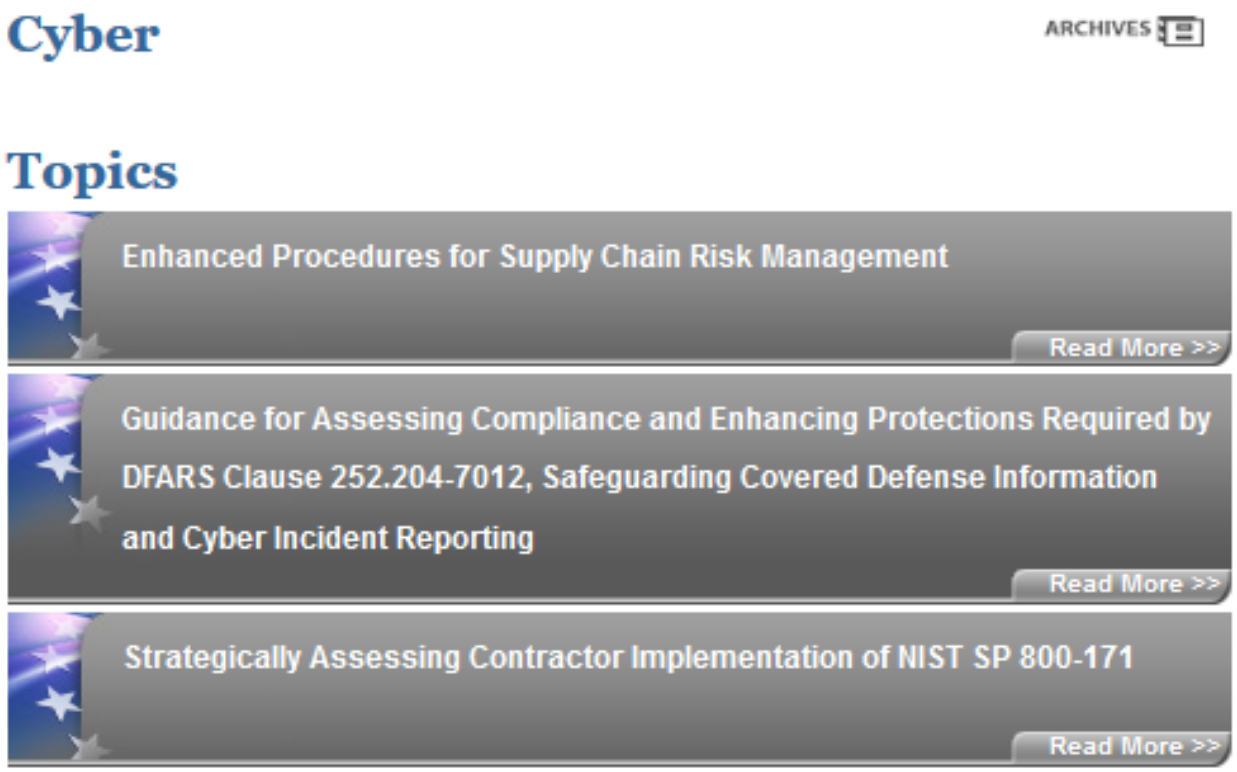


https://dodprocurementtoolbox.com/

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."

Defense Pricing and Contracting



https://www.acq.osd.mil/dpap/pdi/cyber/index.html

Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented
- Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System
- Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base
- Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review
- Strategically Implementing Cybersecurity Contract Clauses

https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html

Somethings to watch for

- CMMC v1.0 is still being referred to as “Draft” v1.02 in process
  - Are there changes in progress
- CMMC v1.X applies to programs, processes and procedures
  - This is being referred to as Phase I
- CMMC Phase II – will apply to hardware
- Foreign governments and other Agencies have expressed interest in the MM
  - Note: DOE is on their CMMC version 2

Additional items to watch for

- NIST released SP – Privacy
- Note, there are three FAR clauses that address Privacy
- Will Privacy be included into CMMC?

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

- April 24, 2020

  How the CyberSecurity Maturity Model Certification (CMMC) Will Impact Your Business
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- April 29, 2020

  Economic Espionage – Awareness of Threats & Resources for Gov't Contractors
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- May 5, 2020

  Learning About the Surety Bond Guarantee from the US SBA
  CLICK HERE for additional information
  Presented by the US Small Business Administration

- May 19, 2020

  Pieces of the Proposal Puzzle
  CLICK HERE for additional information
  Presented by Helen Henningsen, Wisconsin Procurement Institute (WPI)

ACQUISITION HOUR LIVE WEBINARS SERIES

- May 20, 2020

  The Procurement Integrated Enterprise Environment (PIEE) and Wide Area Workflow (WAWF)
  CLICK HERE for additional information
  Presented by the Benjamin Blanc, Wisconsin Procurement Institute (WPI)

- May 29, 2020

  How the CyberSecurity Maturity Model Certification (CMMC) Will Impact Your Business
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- June 9, 2020

  Intellectual property for Government Contractors and Subcontractors and the STTR/SBIR Stakeholder
  CLICK HERE for additional information
  Presented by Laura Grebe, Husch Blackwell

- June 10, 2020

  Negotiation Strategies in Federal Contracting
  CLICK HERE for additional information
  Presented by Helen Henningsen, Wisconsin Procurement Institute (WPI)

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

…More at wispro.org/events

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

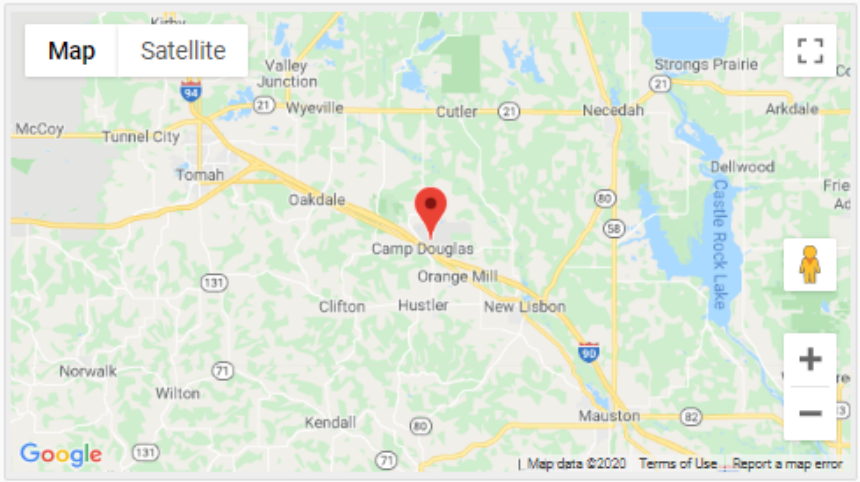
Email:
hilaryd@wispro.org

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



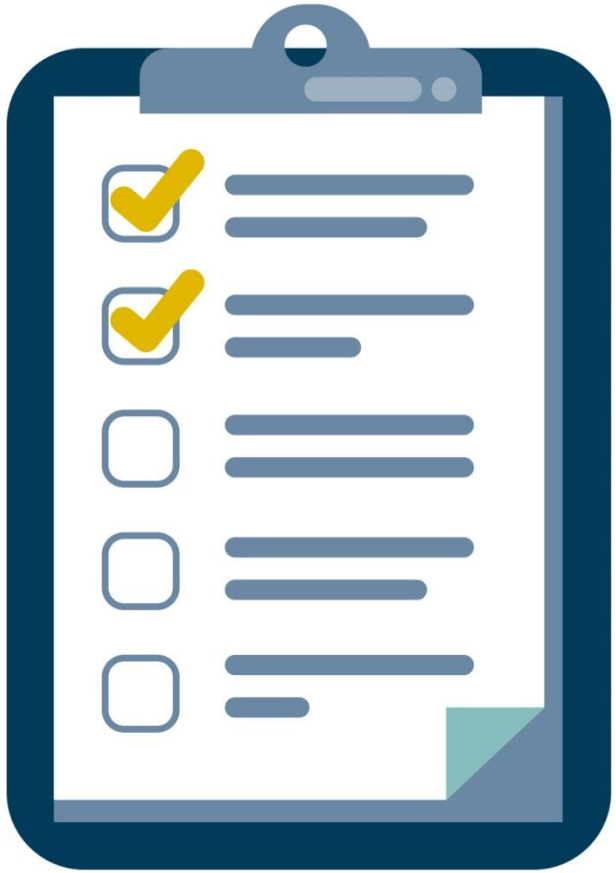
A CRITICAL NOTICE FROM WPI

- If you are a current **FEDERAL / DOD CONTRACTOR or SUBCONTRACTOR** – you may have **CYBER – DATA SECURITY REQUIREMENTS** in your contract.
- If you are responding to any **CURRENT FEDERAL SOLICITATIONS** - be aware of your obligations:
  - Key clauses are 52.204-21, 252.204-7008 and 252.204-7012
  - Review for other possible requirements
- If you are a **DOD CONTRACTOR or SUBCONTRACTOR** – you will have new **CYBER COMPLIANCE – CERTIFICATION REQUIREMENTS** that may impact your business as early as the end of this calendar year.
  - See: https://www.acq.osd.mil/cmmc and https://www.cmmcab.org for more up to date information.
  - *Contact Marc Violante at WPI - marcv@wispro.org or 920-456-9990*

QUESTIONS?

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226