Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

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

## Acquisition Hour Webinar

June 26, 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.

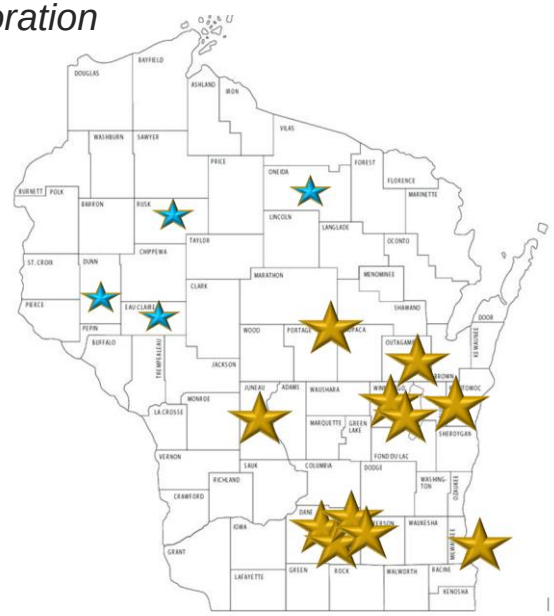
- **INDIVIDUAL COUNSELING – At our offices, at clients facility or via telephone/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

**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

June 26, 2020

# Importance of understanding the drivers!

# Background

## Why agencies need to prevent a classified spillage

In July, the Department of Defense's Inspector General (IG) released a report detailing whether contractors took adequate security measures to protect DoD information. The report found several issues, including a specific incident in which neither the Defense Threat Reduction Agency nor a contractor involved addressed the "spillage of classified information to unclassified cloud, internal contractor network and webmail environments … As a result, classified information remained unprotected on the commercial cloud and the webmail server for almost two years."

This incident is what's known as classified spillage, and it's a major focus for agencies and contractors that are responsible for protecting our national interests. It's also one of the reasons that led the DoD to establish the Cybersecurity Maturity Model Certification (CMMC), which is a set of standards for implementing cybersecurity for defense contractors.

From <https://www.fifthdomain.com/opinion/2020/05/24/why-agencies-need-to-prevent-a-classified-spillage/>

https://www.fifthdomain.com/opinion/2020/05/24/why-agencies-need-to-prevent-a-classified-spillage

# Billion-Dollar Secrets Stolen

- When scientist Hongjin Tan resigned from the Oklahoma petroleum company he'd worked at for 18 months, he told his superiors that he planned to return to China to care for his aging parents. He also reported that he hadn't arranged his next job, so the company agreed to let him to stay in his role until his departure date in December 2018.
- But Tan told a colleague a different story over dinner.
- That conversation prompted Tan's employer to ask him to leave the firm immediately—and then his employer made a call to the FBI tip line to report a possible crime. The resulting investigation led to Tan's guilty plea and 24-month prison sentence for stealing proprietary information that belonged to his company.
- *Tan's theft of a trade secret—one worth an estimated $1 billion—is an example of what the FBI says is a systematic campaign by the Chinese government to gain economic advantage by stealing the innovative work of U.S. companies and facilities.*

FBI agents said he began accessing these sensitive files around the time he applied to China's Thousand Talents Program. U.S. intelligence agencies have found that, through this program, China provides financial incentives and other privileges to participants who are willing to send back the research and technology knowledge they can access while working in the United States.

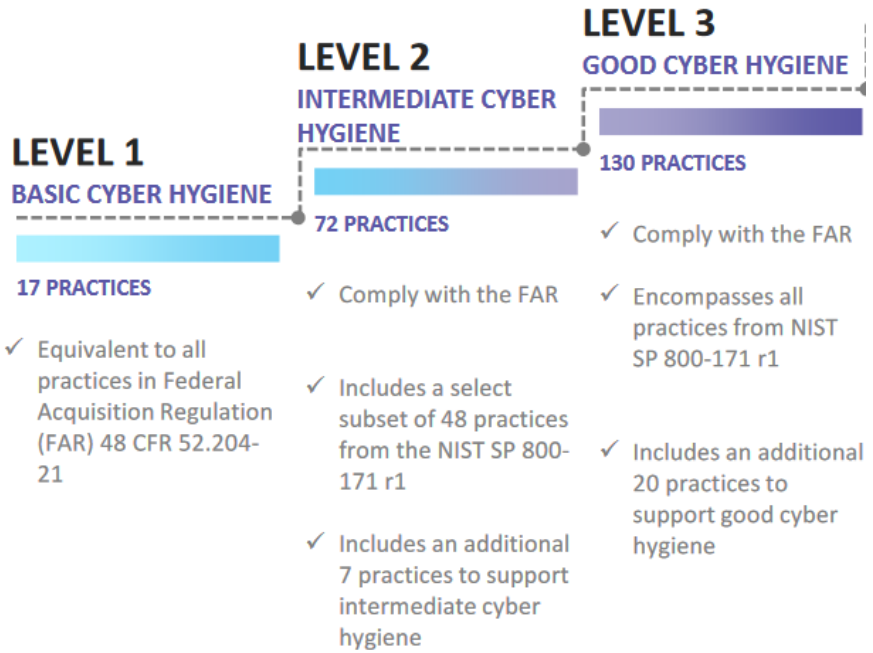
https://www.fbi.gov/news/stories/scientist-sentenced-for-theft-of-trade-secrets-052720

# Leakage – heat loss or information loss?

Copied from Google search: infrared heat loss image

# Current requirement = building blocks

- The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- The intent is for certified independent 3rd party organizations to conduct audits and inform risk.




https://www.acq.osd.mil/cmmc/index.html
https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf slide 7

# 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

# (Why 7008?)The importance of 252.204-7008

- (1) **By submission of this offer, the Offeror represents that it** will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (see http://dx.doi.org/10.6028/NIST.SP.800-171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.

DFARS 252.204-7008 (c)1

# 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.

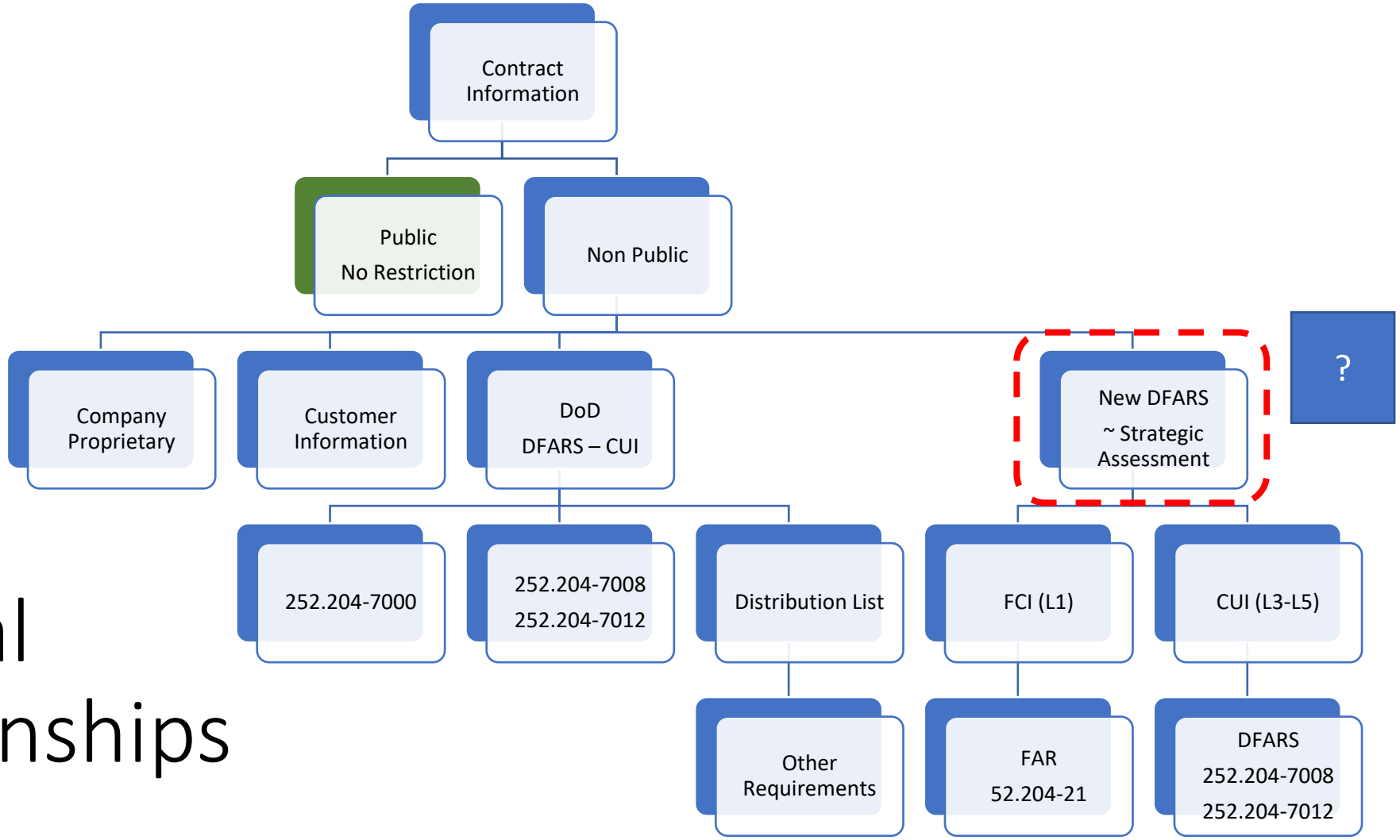
# Information Security Obligations/Requirements – active Today

- 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

# Information Security – items of note

- Public Domain – unrestricted
- Federal Contract Information (FCI)
- Controlled Unclassified Information (CUI)
- Export Controlled
- International Traffic in Arms Regulations (TIAR)
- Joint Certification Program (JCP)
- Export Administration Regulations (EAR)
- Distribution Statement
- NOFORN
- Corporate – internal/proprietary
- Customer/contract - proprietary
- Other

# General Relationships



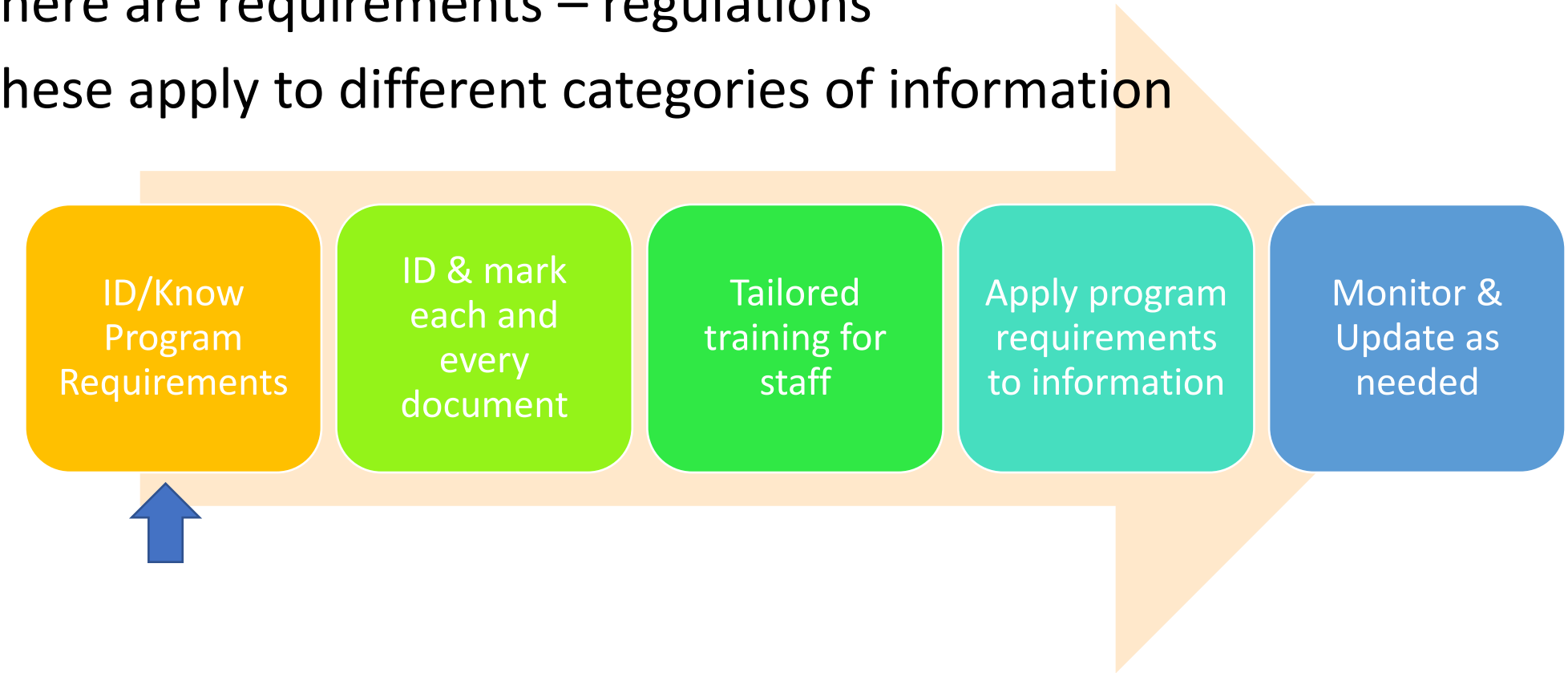
# New DFARS

| | | | |
|---|---|---|---|
| 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. | 04/24/2020 DARS Regulatory Control Officer submitted draft proposed DFARS rule to OIRA. OIRA reviewing. |

https://www.acq.osd.mil/dpap/dars/opencases/dfarscasenum/dfars.pdf Open DFARS Cases as of June 22, 2020 – page 8 of 14

# Commonalities

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



# 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

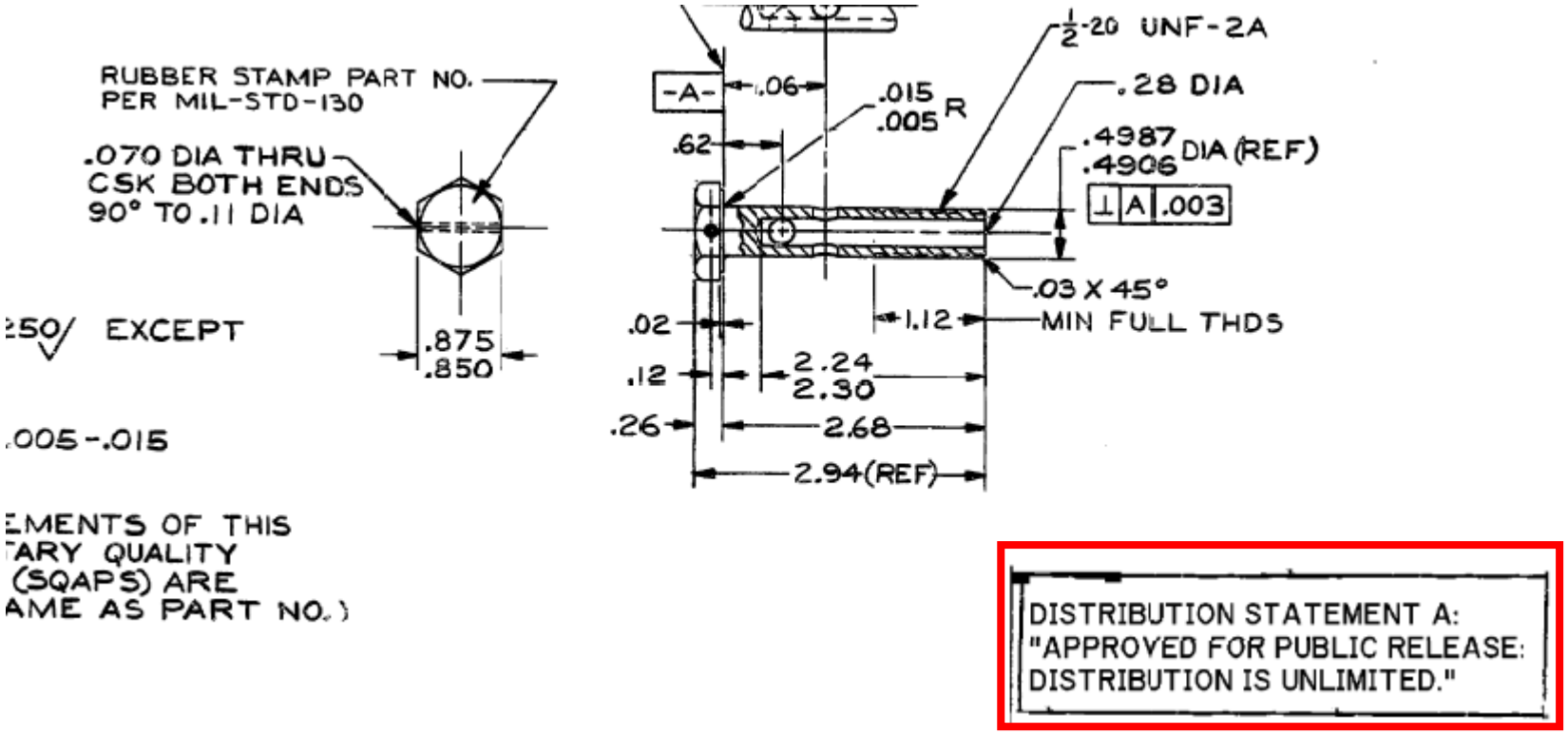
(a) Definitions. As used in this clause-

"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

# 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

# Suggestion – if in doubt – ask questions

- **L.8– Factor I – Cyber Security (Volume 1)**
- The proposal shall address, at a minimum, the offeror's adherence to the following:
  - The primary goal of the proposal submission for the Cyber Security factor is for the offeror to agree to adhere to the government's requirements in accordance with Defense Logistics Acquisition Directive (DLAD) Part 4, Administrative Matters Subpart 4.73-Safeguarding Covered Defense Information and Cyber Incident Reporting. This factor will ensure that the Contractor acknowledges their ability to follow and comply with all National Institute of Standards and Technology (NIST) policies of the FSG 53 acquisition.

  - *Furthermore, this factor will confirm that the Contractor agrees that at the time the Department of Defense (DoD) imposes the new Cybersecurity Maturity Model Certification (CMMC) process, that they will comply with the policy and secure the required certification, regardless of the potential that the new policy may not require active DoD contract holders to comply. The Government reserves the right to review contract NIST compliancy, which may require additional documentation during contract performance.*

https://beta.sam.gov/opp/7401067ce8934b8a972ba2f3ea1b4f37/view?keywords=SPE4A520R0150

# CMMC – How much information to expect?

- Some thoughts
  - CMMC v1.2 is published
  - DFARS 252.204-7012 is current
  - DFARS "Strategic Assessment" – draft rule, one step in the process
  - 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 – what about the "assessment?"
- 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?

# CMMC (FCI v. CUI) – important details

**Federal Contract Information (FCI)**

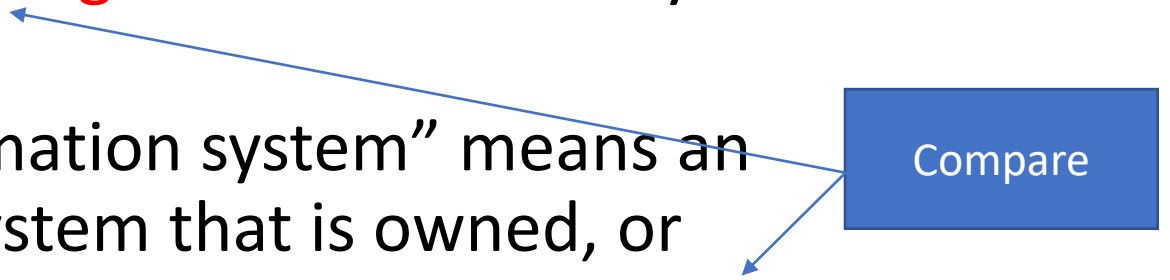
- FAR 52.204-21
  - 15 FAR elements map to 17 CMMC elements
  - Flowdown – substance of clause
- CMMC v1.2

**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

# CMMC – DoD's perspective

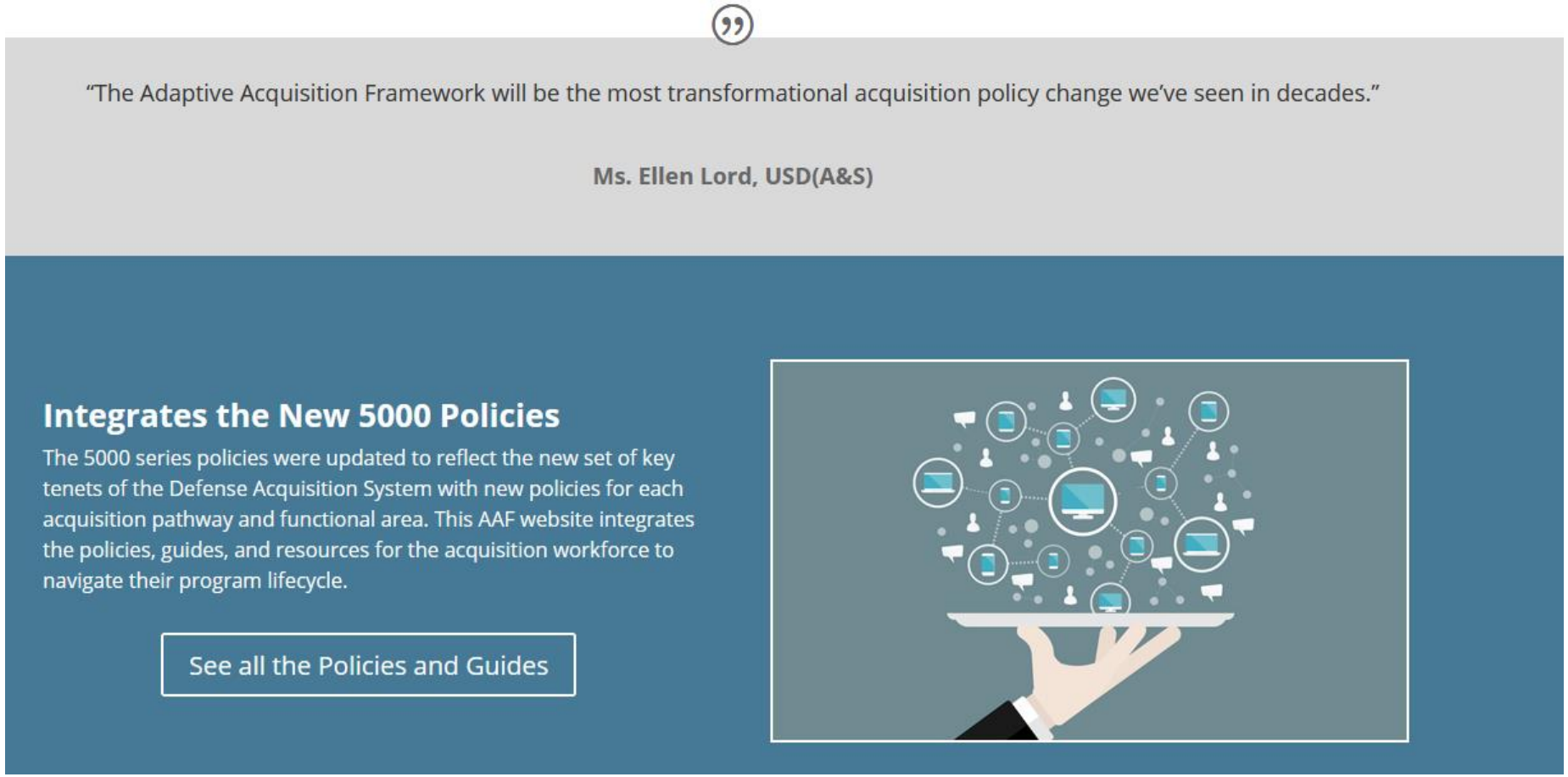
The CMMC is outlined for our program managers in DOD instruction 5000.CSA, the new adaptive acquisition framework. The CMMC is also influencing program protection plans and DoDI 80 -- 8500.01 and 8510.01, which both focus on the protection of I.T. and information systems.

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

# Adaptive Acquisition Framework & the 5000 series






https://aaf.dau.edu/

# Adaptive Acquisition Framework & the 5000 series



| | | |
|---|---|---|
| **DODI 5000.XX**<br>**Engineering**<br>Coming Soon | **DODI 5000.UF**<br>**Test and Evaluation**<br>Coming Soon | **DODI 5000.XX**<br>**Cybersecurity**<br>Coming Soon |
| **DODI 5000.UE**<br>**Mission Engineering**<br>Coming Soon | **DODI 5000.73**<br>**Cost Analysis Guidance and Procedures**<br>Mar 2020 | **DODI 5010.44**<br>**Intellectual Property**<br>Oct 2019 |
| **DODI 5000.XX**<br>**Technology and Program Protection**<br>Coming Soon | **DODI 5000.82**<br>**Acquisition of Information Technology**<br>Apr 2020 | **DODI 5000.UD**<br>**Acquisition Intelligence**<br>Coming Soon |
| **DODD 5000.71**<br>**Rapid Fulfillment of UONs**<br>Aug 2018 | **DODI 5000.XX**<br>**Human Systems Integration**<br>Coming Soon | **All DODIs**<br>**WHS Executive Services Directorate** |

https://aaf.dau.edu/

# Important Change

# 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

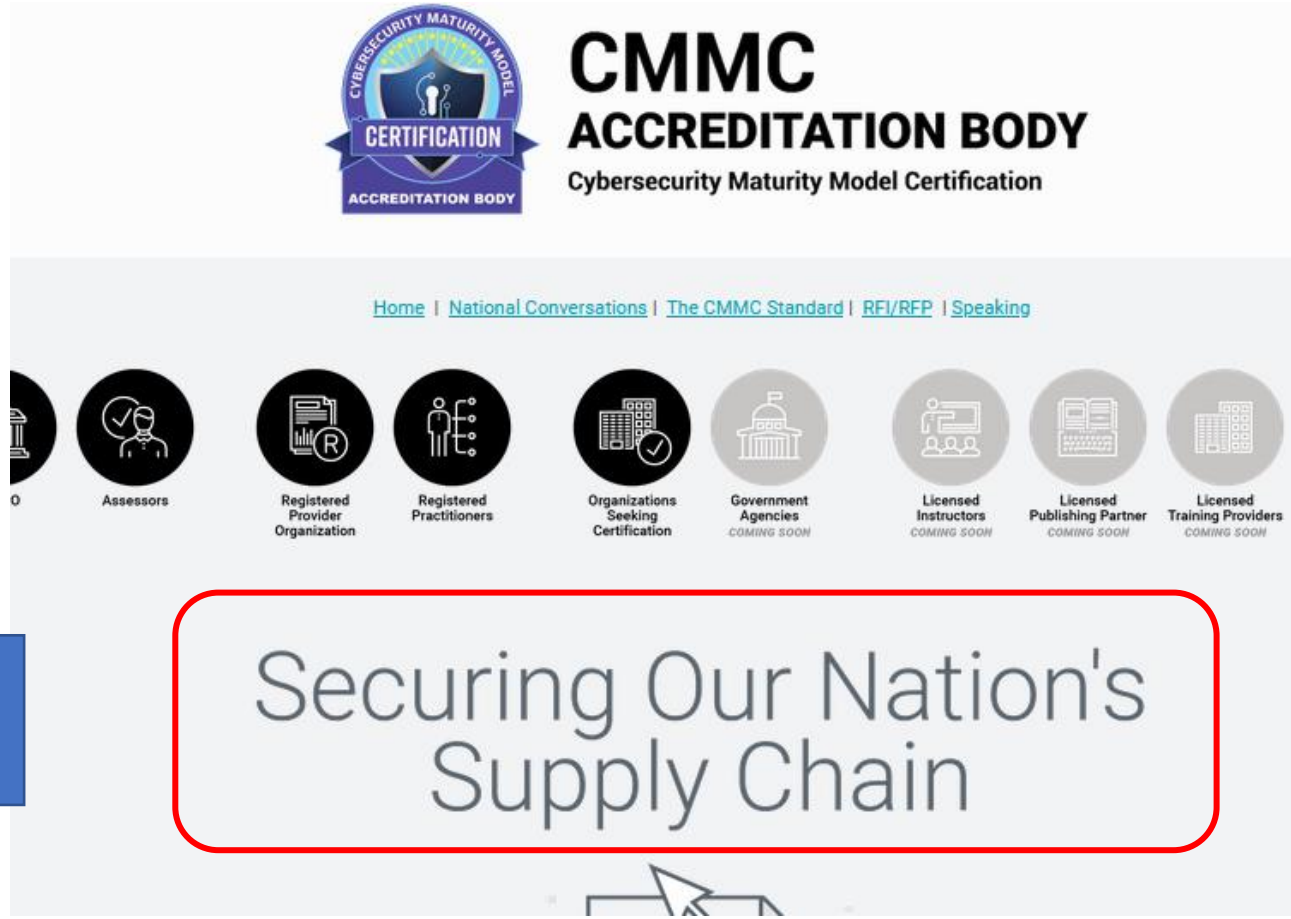
# The desired end state

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


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

# Interesting – subtle change




Used to use DIB – Defense Industrial Base

https://www.cmmcab.org/

# 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."

# 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 (CMMC FAQ's)*
  - 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

# Source for CMMC Practices Per Level

| CMMC Level | Number of Practices Introduced at CMMC Level | Source | | | |
|---|---|---|---|---|---|
| | | 48 CFR 52.204-21 | NIST SP 800-171r1 | Draft NIST SP 800-171B | Other |
| 1 | 17 | 15* | 17* | – | – |
| 2 | 55 | – | 48 | – | 7 |
| 3 | 58 | – | 45 | – | 13 |
| 4 | 26 | – | – | 11 | 15 |
| 5 | 15 | – | – | 4 | 11 |
| **Total** | **171** | **15** | **110** | **15** | **46** |

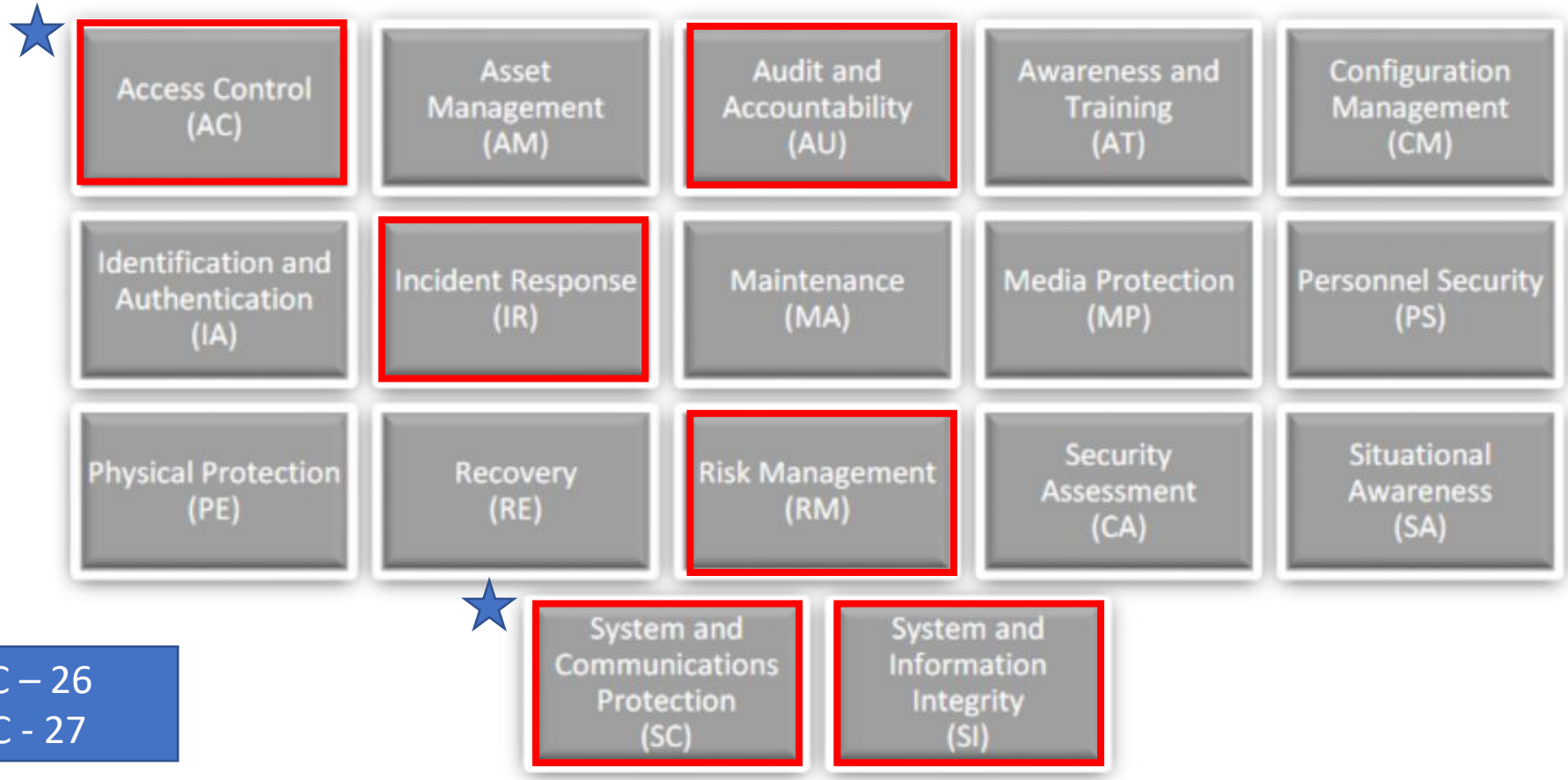
*Note: 15 safeguarding requirements from 48 CFR 52.204-21 correspond to 17 security requirements in NIST SP 800-171.

# CMMC – a pareto perspective

| | |
|---|---|
| Access Control (AC) | • Establish system access requirements<br>• Control internal system access<br>• Control remote system access<br>• Limit data access to authorized users and processes |
| Systems and Communications Protection (SC) | • Define security requirements for systems and communications<br>• Control communications at system boundaries |

https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf Table 1, page 8

# The “Big Six” (105 of 171 practices)




AC – 26
SC - 27

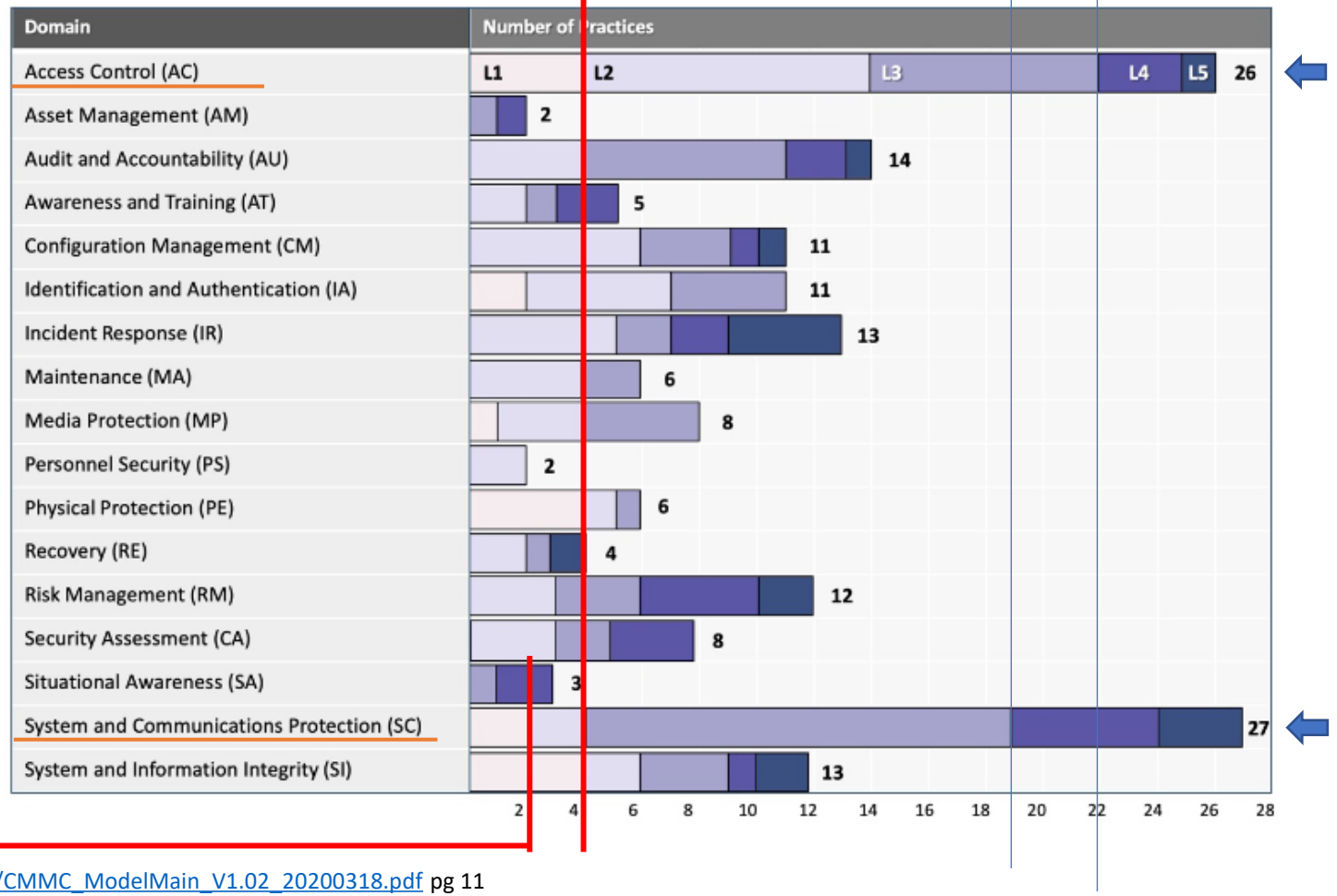
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf pg 11

# Practices v. Domain v. Level

SC: L3 - 19

AC: L1 - 4

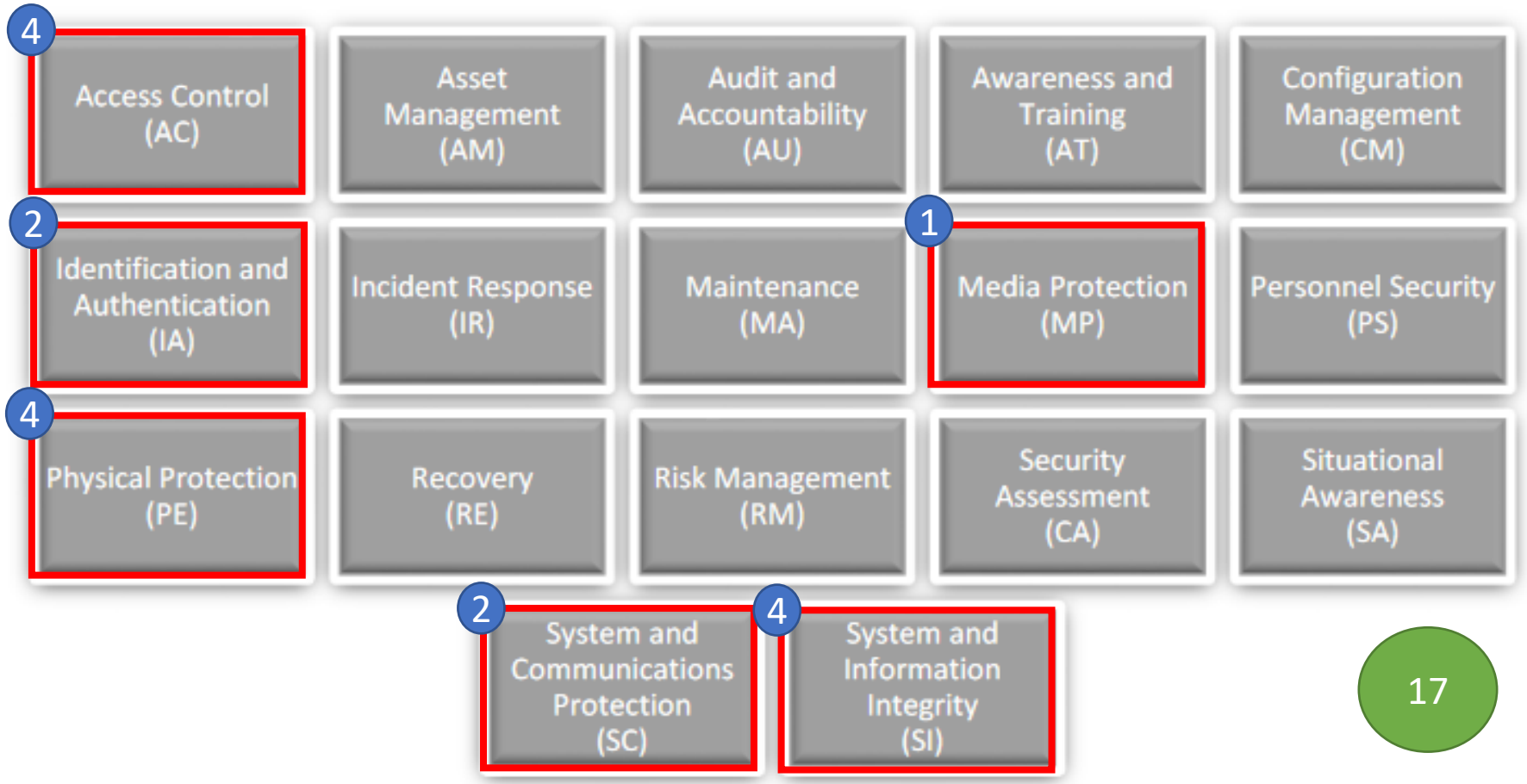
AC: L3 - 22




SC: L1 - 4

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

# CMMC – Domains (Level-1)



# C001- Establish system access requirements –a

- AC.1.001
  Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
  - FAR Clause 52.204-21 b.1.i
  - NIST SP 800-171 Rev 1 3.1.1
  - CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11
  - NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4
  - CERT RMM v1.2 TM:SG4.SP1
  - NIST SP 800-53 Rev 4 AC-2, AC-3, AC-17
  - AU ACSC Essential Eight

# 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

# C001- Establish system access requirements – a1

- FAR Clause 52.204-21 b.1.i

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

- NIST SP 800-171 Rev 1 3.1.1

### 3.1 ACCESS CONTROL

*Basic Security Requirements*

3.1.1 Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

| 3.1.1 | **SECURITY REQUIREMENT**<br>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). |
|---|---|
| | **DISCUSSION**<br>Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for both systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged verses non-privileged) are addressed in requirement 3.1.2. |

SPECIAL PUBLICATION 800-171 PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS REVISION 1 – Left: pg 9 | Right: Appendix F, pg 69

# C001- Establish system access requirements – a2

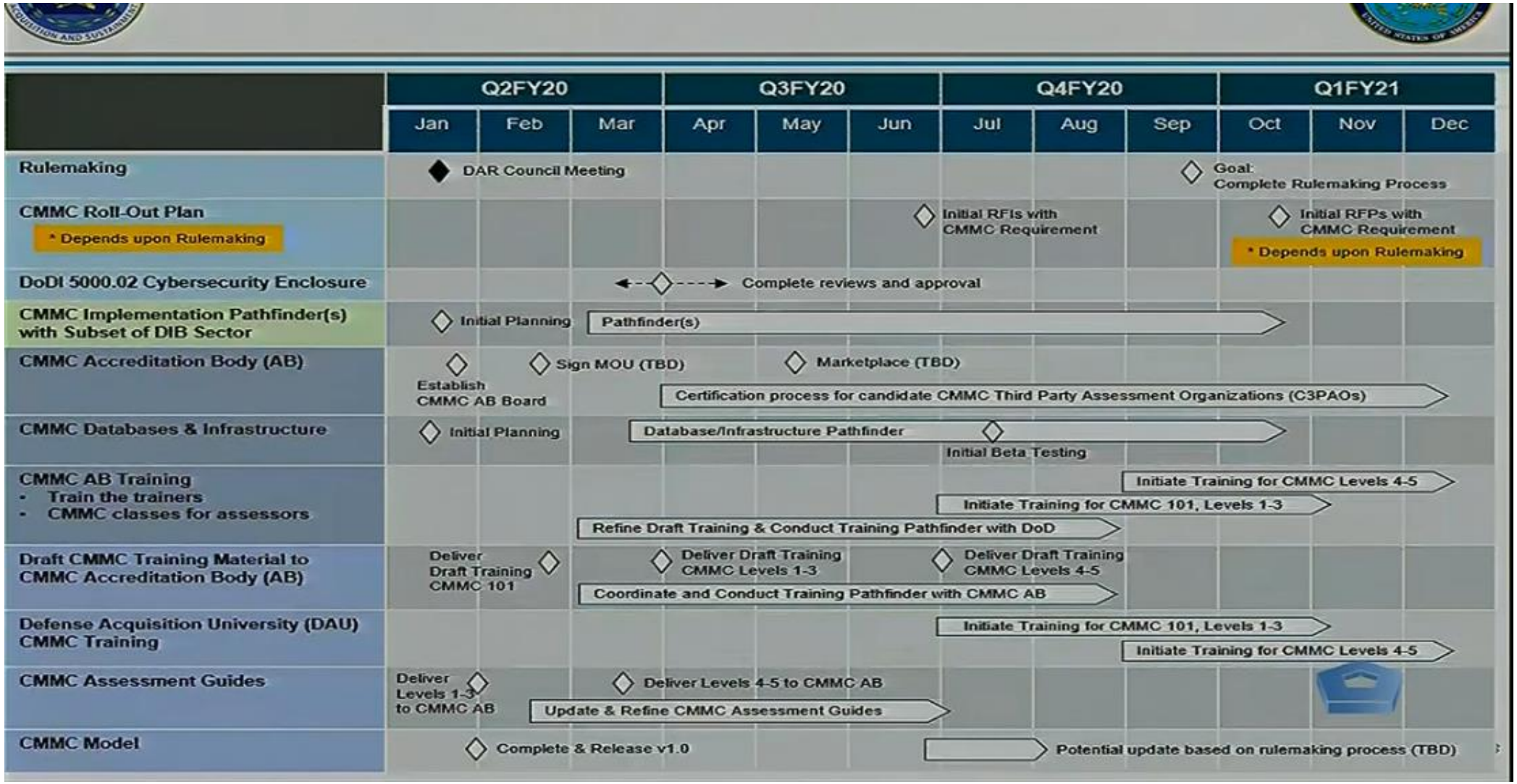
| 3.1.1 | **SECURITY REQUIREMENT**<br>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). | |
|---|---|---|
| | **ASSESSMENT OBJECTIVE**<br>*Determine if:* | |
| | **3.1.1[a]** | *authorized users are identified.* |
| | **3.1.1[b]** | *processes acting on behalf of authorized users are identified.* |
| | **3.1.1[c]** | *devices (and other systems) authorized to connect to the system are identified.* |
| | **3.1.1[d]** | *system access is limited to authorized users.* |
| | **3.1.1[e]** | *system access is limited to processes acting on behalf of authorized users.* |
| | **3.1.1[f]** | *system access is limited to authorized devices (including other systems).* |
| | **POTENTIAL ASSESSMENT METHODS AND OBJECTS**<br>**Examine**: [*SELECT FROM:* Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].<br>**Interview**: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].<br>**Test**: [*SELECT FROM:* Organizational processes for managing system accounts; mechanisms for implementing account management]. | |

NIST SP 800-171A ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION – pg 9

# C001- Establish system access requirements – a3

- CIS Controls v7.1 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11
  - 1.4 Devices Identify Maintain Detailed Asset Inventory Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.
  - 1.6 Devices Respond Address Unauthorized Assets Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.
  - 5.1 Applications Protect Establish Secure Configurations Maintain documented security configuration standards for all authorized operating systems and software.
  - CIS Controls -- 14.6, 15.10, 16.8, 16.9, 16.11 – not shown

https://www.cisecurity.org/controls/ - Excel Download




Timeline charge from January 31, 2020 Press Briefing

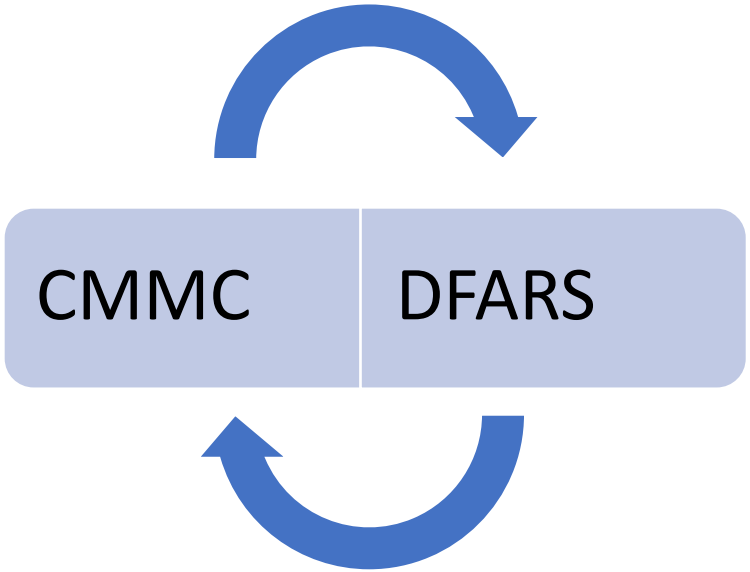
# Major Milestones

- 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.

# 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.



# 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

# Certification – does not happen overnight

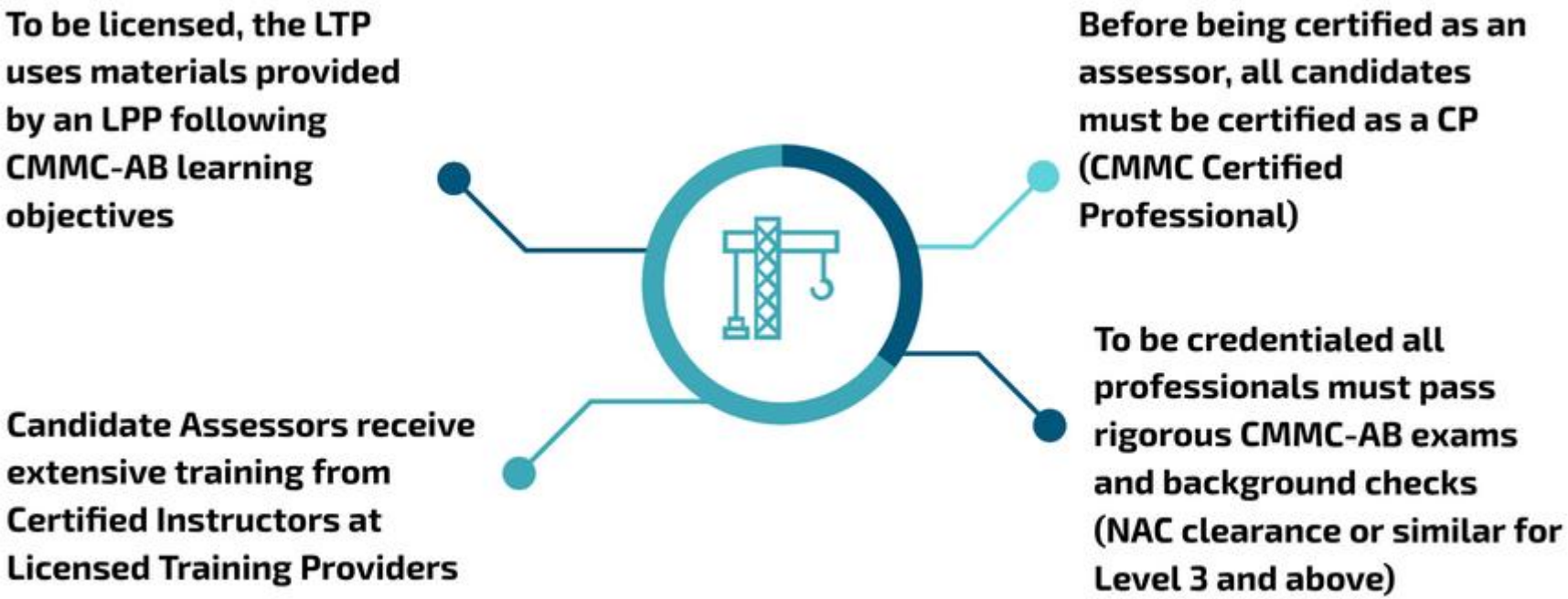

https://www.cmmcab.org Link (icon) Organizations Seeking Certification

# CMMC – planning consideration

**Recognize that by 2025 all DoD Suppliers Need CMMC Certification**

https://www.cmmcab.org Link (icon) Organizations Seeking Certification

# CMMC – Assessment Ecosystem




https://www.cmmcab.org Link (icon) Organizations Seeking Certification

# CMMC – process (In 10 steps)


1. Understand CMM Requirements
2. Identify your scope. Enterprise, Organization Unit or Program Enclave
3. Identify the desired Maturity Level
4. Optional. Pre-assess using an RPO or C3PAO
5. Close any identified gaps.
6. Find a C3PAO on the CMMC-AB Marketplace
7. Conduct Assessment with C3PAO's Certified Assessment Team
8. Allowance of up to 90 days to resolved findings (if any).
9. CMMC-AB reviews submitted assessment.
10. Upon approval, 3 year Certification issued!

https://www.cmmcab.org Link (icon) Organizations Seeking Certification

# CMMC-AB Certification valid period


https://www.cmmcab.org Link (icon) Organizations Seeking Certification

# 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.

# 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.

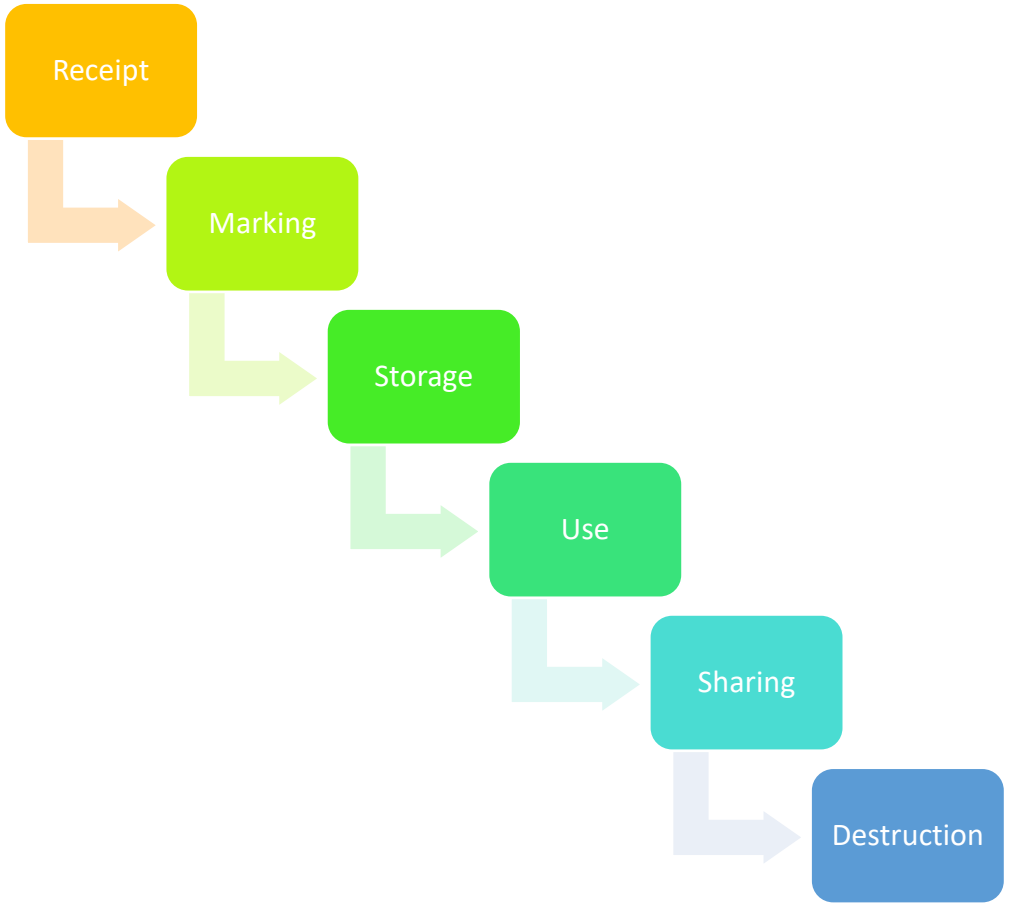
https://www.cmmcab.org/ - mid May, since removed

*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

# Key Elements

# 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

# Utilize references and integrate requirements

**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

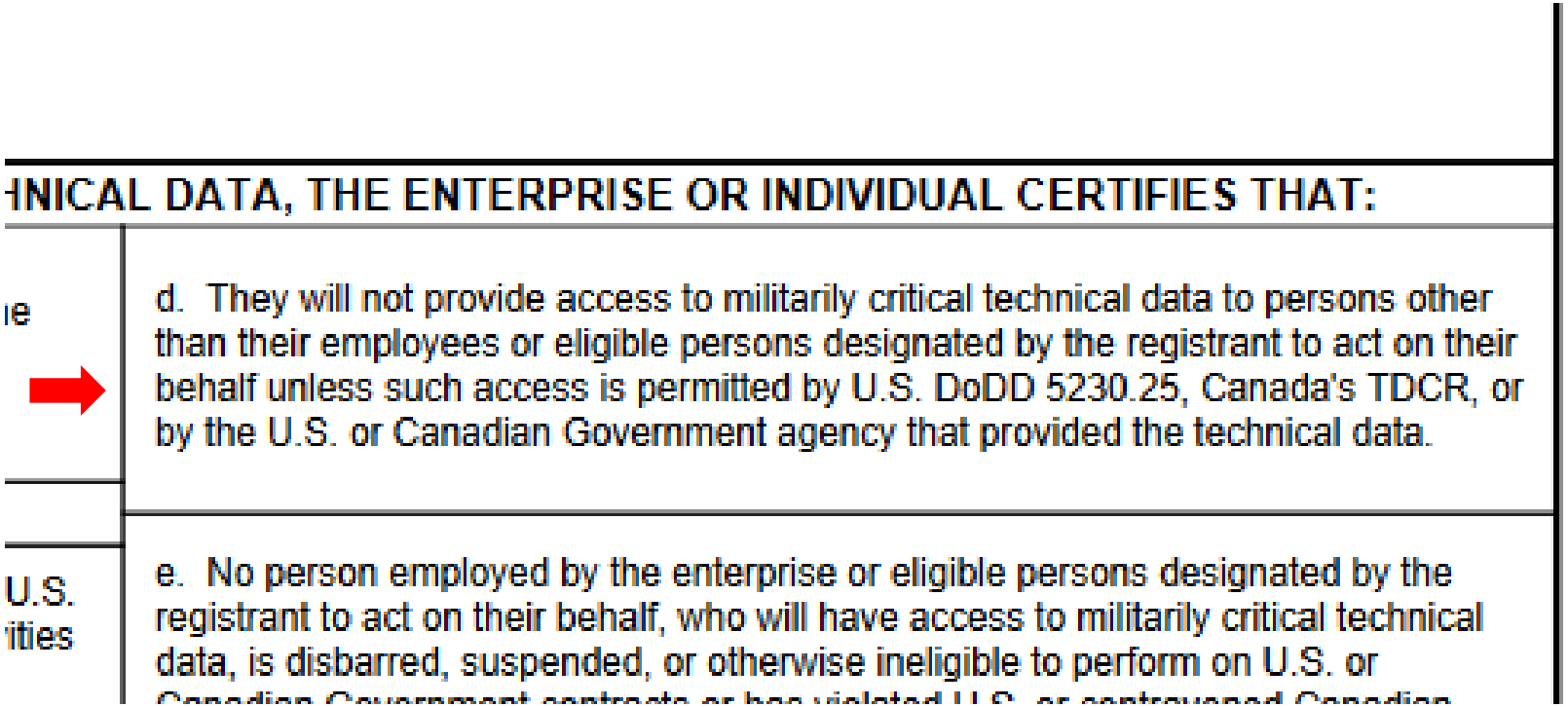
REFERENCES, continued

(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:

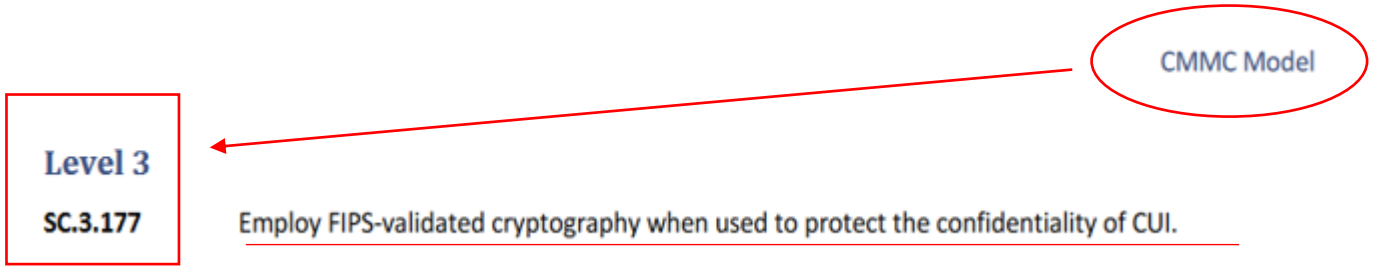
ıe

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 / Definitions

- 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

# 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.

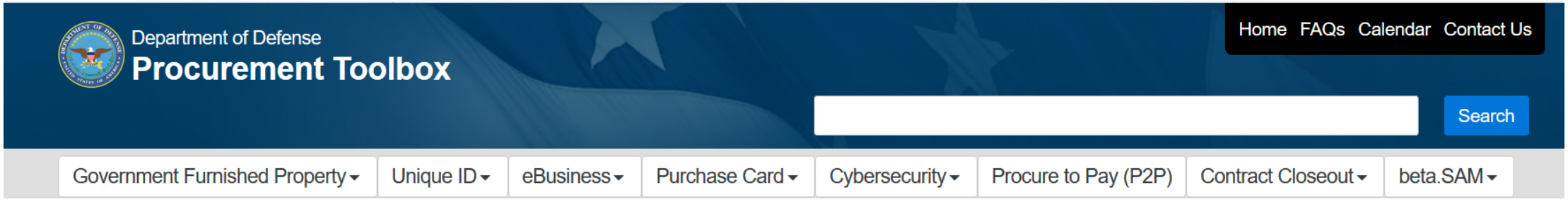
# Office of the Under Secretary of Defense (A&S)


https://www.acq.osd.mil/cmmc/draft.html

# CMMC-AB


https://www.cmmcab.org

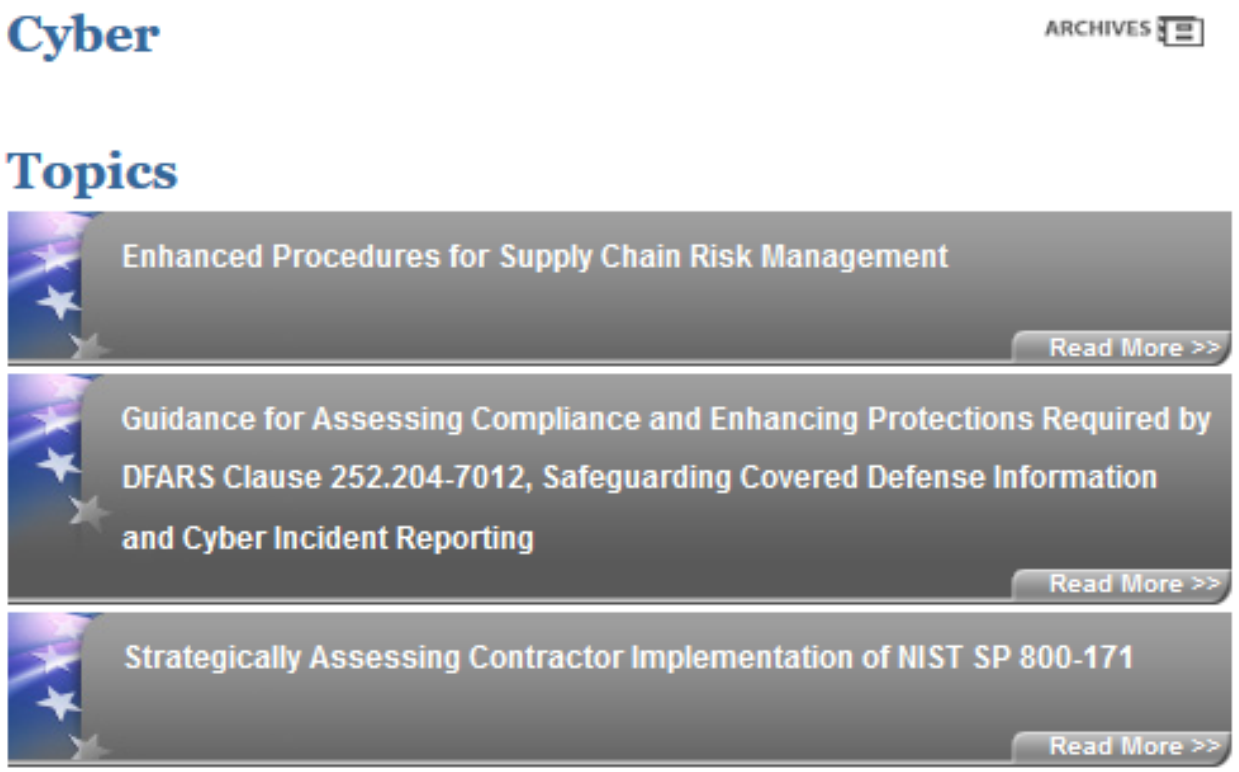
# DoDProcurementtoolbox.com





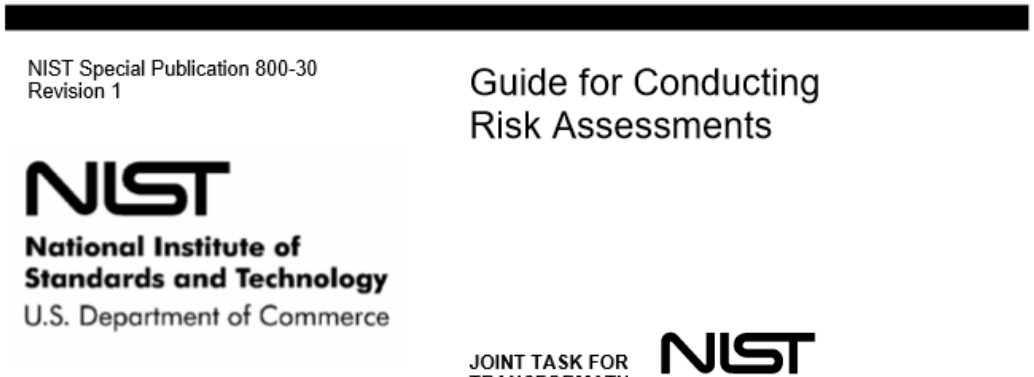
https://dodprocurementtoolbox.com/

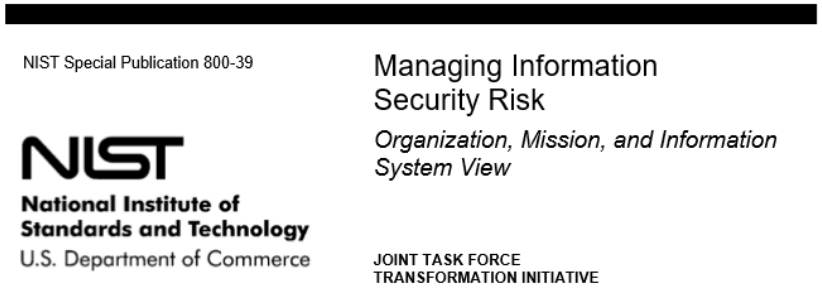
# Defense Pricing and Contracting

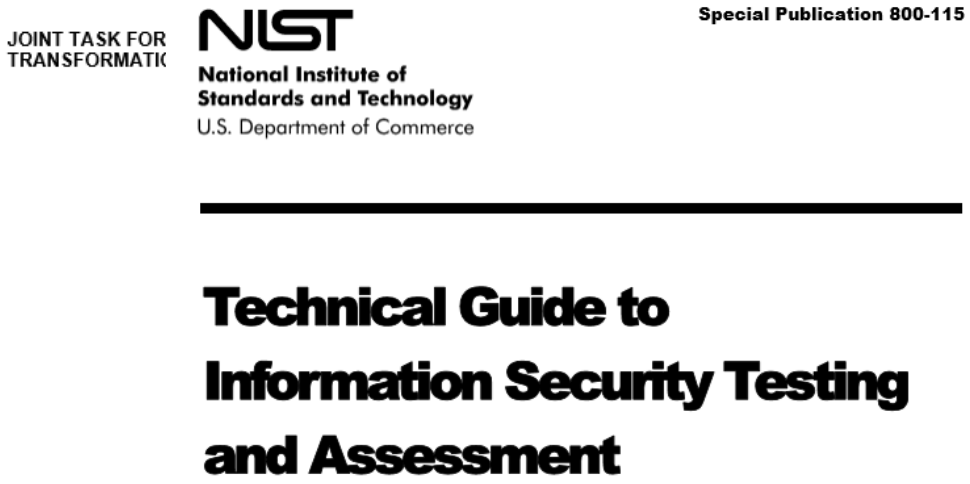



https://www.acq.osd.mil/dpap/pdi/cyber/index.html

# NIST resources

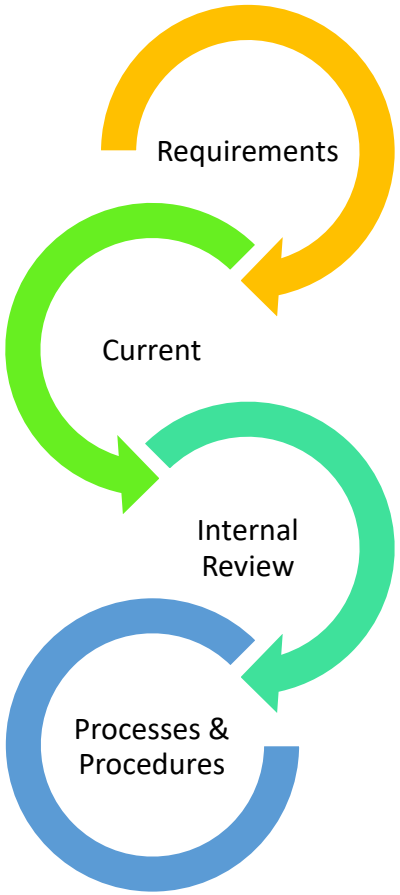



http://csrc.nist.gov/publications.

# Getting to the desired – End State (Resilience)



# 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

# 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

# Implementation References

- FAR 52.204-21 – entirety https://www.acquisition.gov
- NIST 800-171 r1 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final
- NIST 800-171 r2 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-53 Rev 4 - https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final
- NIST CSF v1.1 - https://doi.org/10.6028/NIST.CSWP.04162018
- CERT RMM v1.2 - https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf
- CISecurity Controls - https://www.cisecurity.org/controls/
- AU ACSC Essential Eight - https://www.cyber.gov.au/publications/essential-eight-maturity-model
- UK NCSC Cyber Essentials - https://www.ncsc.gov.uk/cyberessentials/overview

# Just arrived in my in-box

## Third-Party Risk Management Leader Delivers the Industry's First Comprehensive Cybersecurity Maturity Model Certification (CMMC) Standardized Assessments

Prevalent is the only vendor to provide a single platform for auditors and contractors to assess, document and remediate risk across all CMMC domains and practice areas

https://www.wfmz.com/news/pr_newswire/pr_newswire_technology/third-party-risk-management-leader-delivers-the-industrys-first-comprehensive-cybersecurity-maturity-model-certification-cmmc/article_aa0b91b0-1f02-5026-ab65-ab32e9cfcc34.html

# UPCOMING TRAINING - EVENTS

# ACQUISITION HOUR LIVE WEBINARS SERIES

- June 26, 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)

- July 1, 2020

  **ARE YOU READY – BIG Changes coming to the US SBA Federal Women-Owned Small Business Program**
  CLICK HERE for additional information
  Presented by Shane Mahaffy, US Small Business Administration (SBA)

- July 7, 2020

  **Tools and Resources to use for Gaining a Better Understanding of your Federal Customer**
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

- July 14, 2020

  **The SBA 8(a) Certification Program**
  CLICK HERE for additional information
  Presented by Shane Mahaffy, US Small Business Administration (SBA)

# ACQUISITION HOUR LIVE WEBINARS SERIES

- July 15, 2020

  **Responding to Sources Sought and Capabilities Statements**
  CLICK HERE for additional information
  Presented by Mark Dennis, Wisconsin Procurement Institute (WPI)

- July 21, 2020

  **OFCCP Compliance 101**
  CLICK HERE for additional information
  Presented by Roselle Rogers & Tim Muma, LocalJobNetwork

- July 22, 2020

  **The HUBZone Certification Program**
  CLICK HERE for additional information
  Presented by Shane Mahaffy, US Small Business Administration (SBA)

- July 28, 2020

  **The Spend to the End**
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute

- August 25, 2020

  **State and Federal Certifications For Veteran and Service Disabled Veteran Owned Businesses**
  CLICK HERE for additional information
  Presented by Shane Mahaffy, US Small Business Administration (SBA) and Mark Dennis, Wisconsin Procurement Institute (WPI)

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

**…More at wispro.org/events**

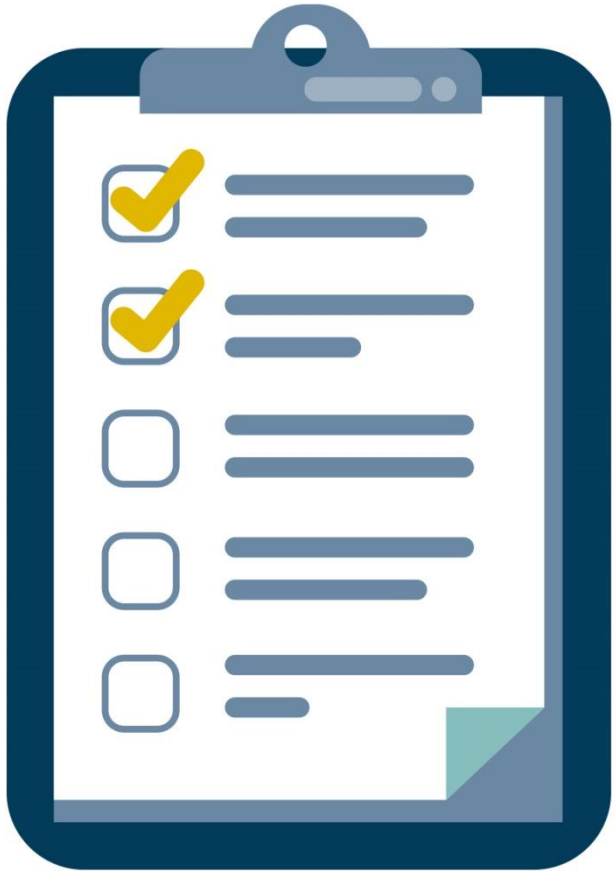
# A CRITICAL NOTICE FROM WPI

- 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



Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

# 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