Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

INTRODUCTION TO CMMC LEVEL 1

Acquisition Hour Webinar

August 14, 2020




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

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

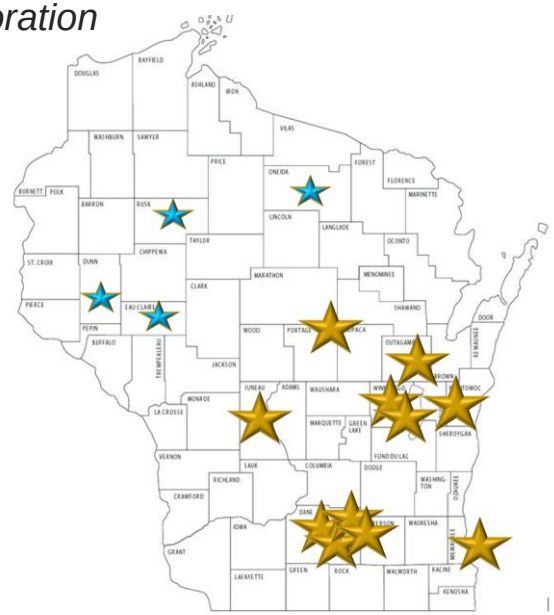
- **INDIVIDUAL COUNSELING – At our offices, at clients facility or via telephone/GoToWebinar**
- **SMALL GROUP TRAINING – Workshops and webinars**
- **CONFERENCES to include one on one or roundtable sessions**

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.

Introduction to CMMC Level 1 requirements

Marc Violante

Wisconsin Procurement Institute

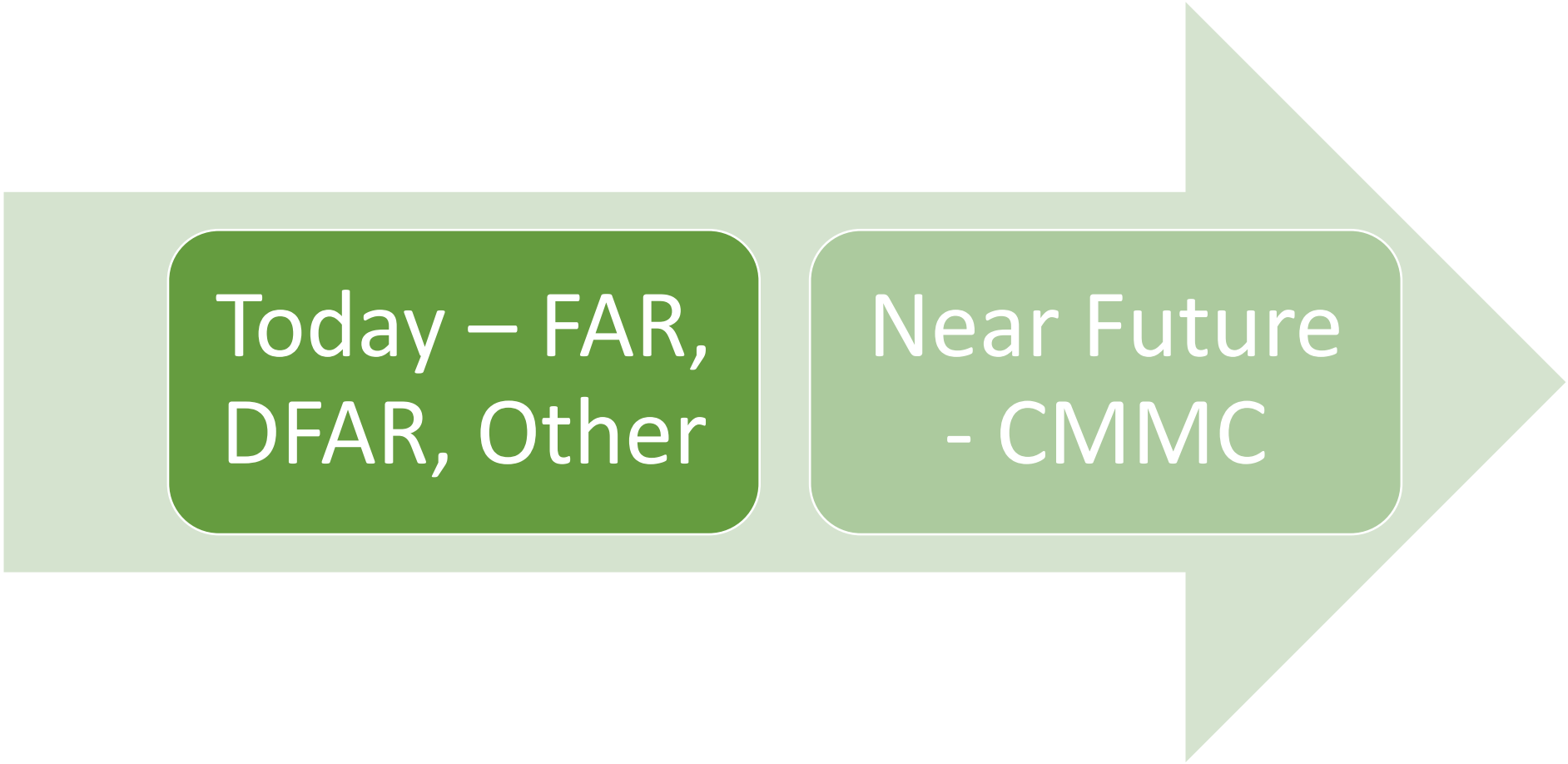
August 14, 2020

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

Today’s goals

- Usable resource(s)
- Background to the need
- Overview of CMMC L1
- Highlight process and entities involved
- Highlight recurring ideas
- Sketch out a path for moving forward

Cyber Requirements



What we know - Current Cyber Obligations

Contractual requirements - today

- 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems (FCI) – 15 elements
- 252.204-7008 - Compliance with safeguarding covered defense information controls
- 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting (CUI)
  - Adequate security | NIST 800-171 r2 | Malware | Incident Id, investigation* & Reporting | "does not abrogate" - requirement
- DON – Geurts memos – CDRL requirements
- Other requirements

*If required – if there has been an incident that meets defined threshold.

Information –general categories -

Federal Contract Information (FCI) = CMMC L1

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. – CDI = CTI and CUI

NOFORN – Intelligence | Navy Nuclear

Distribution List (b-f)

Export Controlled – ITAR | JCP | Other

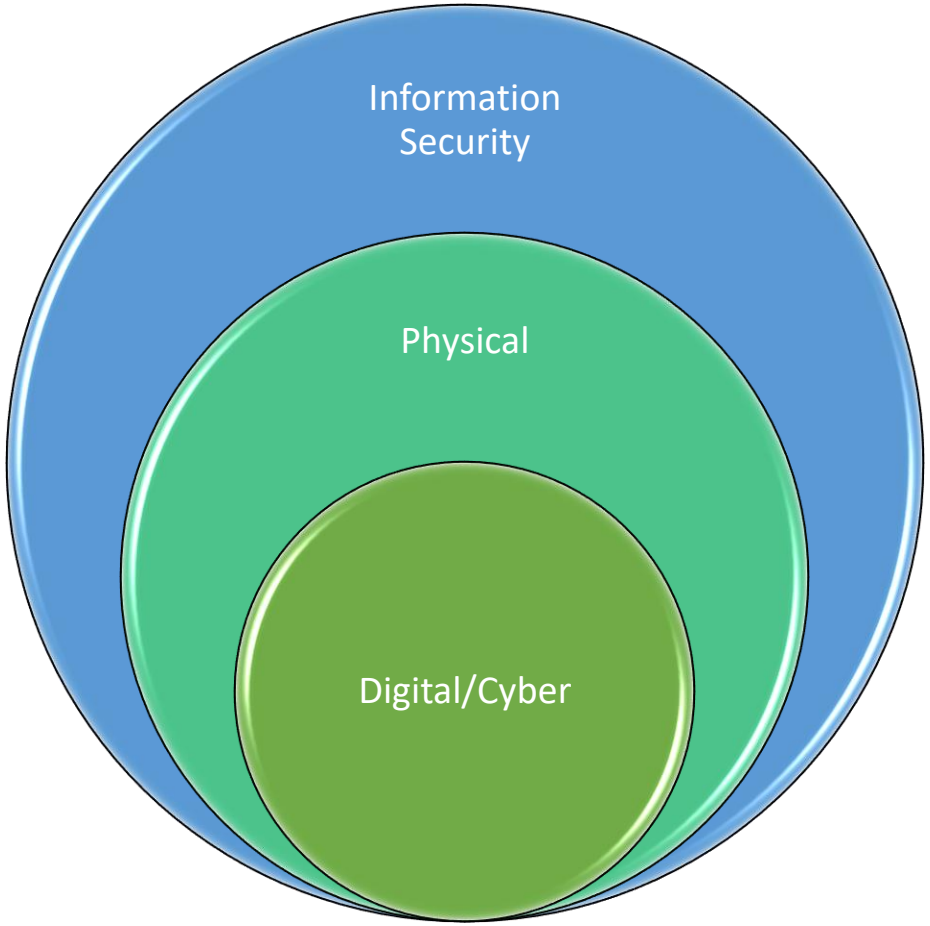
Corporate

Customer

Various categories are used

Publish Date	Type	Code	Description	Keywords	Due Date	
08/07/20	SAM	63	Carbon Nanotube	CUI	2020-08-24	View
08/07/20	SAM	A	Carbon Nanotube	CUI	2020-08-24	View
08/07/20	SAM	Y,Z	Construction Contract for the Customs and Border Protection Seized Cargo Facility	CUI	2020-08-25	View
08/06/20	SAM	13	M28B2 Percussion Primer	DISTRIBUTION, STATEMENT	2020-09-05	View
08/06/20	SAM	58,80	BRUSH,ARTIST	NOFORN	2020-08-18	View
08/06/20	SAM	58,80	BRUSH,ARTIST	NOFORN	2020-08-18	View
08/06/20	SAM	R	BRUSH,ARTIST	NOFORN	2020-08-18	View
08/06/20	SAM	R	BRUSH,ARTIST	NOFORN	2020-08-18	View
08/05/20	SAM	20	HEALY Vibration Monitoring System Mod 03	CONTROLLED, UNCLASSIFIED	2020-09-15	View
08/05/20	SAM	23	Aluminum Trailer per Specifications	CONTROLLED, UNCLASSIFIED	2020-08-14	View
08/04/20	SAM	19	Navy Cable Ship Replacement T-ARC(X)	DISTRIBUTION, STATEMENT	2020-08-31	View
08/04/20	SAM	42,63	7th & 9th Floor GAO Office Renovation, Chicago, IL	CUI	2020-08-10	View
08/04/20	SAM	H	TESTS AND CERTIFICATIONS OF LIGHTNING PROTECTION SYSTEMS, USAG ITALY DMC	CUI	2020-09-03	View
08/04/20	SAM	Z	7th & 9th Floor GAO Office Renovation, Chicago, IL	CUI	2020-08-10	View
07/31/20	SAM	13	120mm Tank Training Ammunition - FY22-FY26	DISTRIBUTION, STATEMENT	2020-08-31	View
07/31/20	SAM	15,23,59	Aircraft Launcher Interface Computer (ALIC) Chassis and Associated Mechanical Assemblies.	CUI	2020-09-07	View
07/31/20	SAM	23	UYX-4 PROCESSOR CHASSIS	DISTRIBUTION, STATEMENT	2020-08-17	View
07/31/20	SAM	48	ACTUATOR,HYDRAULIC-	DISTRIBUTION, STATEMENT	2020-08-04	View
07/31/20	SAM	53	Hardware Manufacturing for CADPAD Programs: M25A1, CKU-5, CCU-22, CCU-68, CCU-93, CCU-94, M1	CUI	2020-08-07	View
07/31/20	SAM	65,66	X-Ray Cabinet Commercial Buy	CUI	2020-08-31	View

Information security v. Cyber



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

Information Security Obligations/Requirements

Equally Important & Related

- 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 (CCL) – Red Flag Questions
- DLA Requirements –
  - DLA Export Control Data Access - JCP

Cyber's relation to other Federal programs

- *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. Para L DFARS 252.204-7012

252.204-7012 (October 2016) Safeguarding Covered Defense Information and Cyber Incident Reporting. Paragraph (l)

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

Without a Secure Foundation All Functions are at Risk

https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf

Issue -

Bottom line, technology theft puts the United States at a disadvantage in its strategic competition with China and Russia, the general said.

https://www.defense.gov/Explore/News/Article/Article/2027555/task-force-curbs-technology-theft-to-keep-joint-force-strong/

Protecting Critical Technology Task Force

- “The task force's beginnings date back about four years, when a nation stole technology after hacking into a company's computer network, Murphy said. Which nation and what technology aren't relevant — what is relevant is that DOD didn't find out about the loss for over a year, he said.”

https://www.defense.gov/Explore/News/Article/Article/2027555/task-force-curbs-technology-theft-to-keep-joint-force-strong/ Nov 29, 2019

Small Business risk – “it won’t happen to us”

- It’s not just Fortune 500 companies and nation states at risk of having IP stolen–even the local laundry service is a target.
- In one example, an organization of 35 employees was the victim of a cyber attack by a competitor.
- The competitor hid in their network for two years stealing customer and pricing information, giving them a significant advantage.

Hid for two years!

Internet Security Threat Report, Volume 21, April 2016, Symantec

Information is a powerful driver!

Copied from http://www.agriculture.com/news/business/chinese-nationals-charged-with-stealing_5-ar36216

Why?

Northern District of New York

FOR IMMEDIATE RELEASE

Tuesday, April 23, 2019

Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets

The Pair Allegedly Conspired to Steal GE's Trade Secrets for Use in Their China-Based Companies to Benefit the People's Republic of China

"The indictment alleges a textbook example of the Chinese government's strategy to rob American companies of their intellectual property and to replicate their products in Chinese factories, enabling Chinese companies to replace the American company first in the Chinese market and later worldwide," said Assistant Attorney General Demers. "We will not stand idly by while the world's second-largest economy engages in state-sponsored theft. As part of the Attorney General's China Initiative, we will partner with the private sector to hold responsible those who violate our laws, and we urge China's leaders to join responsible nations and to act with honesty and integrity when competing in the global marketplace."

https://www.justice.gov/usao-ndny/pr/former-ge-engineer-and-chinese-businessman-charged-economic-espionage-and-theft-ge-s

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

What we don't know about the CMMC

- New DFARs (replace/modify – 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 v1.2
  - 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

*Level 1 does not specify documentation but…?

Open DFARS Cases as of July 27, 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.	04/24/2020 DARS Regulatory Control Officer submitted draft proposed DFARS rule to OIRA. OIRA reviewing.

Interesting terms –

- Strategic Assessment
- Measures institutionalization – practices and processes
- Partially implements section 1648 of the FY20 NDAA

DoD Press Release – Monday, June 1, 2020

- Announced – DoD / CMMC-AB MOU
  - established the roles, responsibilities, and authorities of each organization to help ensure a cyber-safe, cyber-secure and cyber-resilient defense industrial base.
  - Delay due to Covid response
- *The MOU states that DoD will only accept certifications from an assessor or a CMMC Third Party Assessment Organization (C3PAO) who has been accredited for assessments by the CMMC-AB.*

https://www.defense.gov/Newsroom/Releases/Release/Article/2204213/dod-signed-memorandum-of-understanding-with-cybersecurity-maturity-model-certif/source/GovDelivery/

With respect to Third Parties

CMMC Third Party Assessment Organizations (C3PAOs) and CMMC Training

- The Department is aware that some entities have made claims of being able to provide CMMC certifications for the purposes of contracting with the DoD. The requirements for becoming a CMMC Third Party Assessment Organization (C3PAO) are not yet established. As a result, there are no third-party entities at this time that have been credentialed to conduct a CMMC assessment which will be accepted by the CMMC Accreditation Body. Similarly, at this time, only training materials or presentations provided by the Department will reflect the Department's official position with respect to the CMMC program.

The Sources!

CMMC Model overview briefing:

CMMC Model Briefing PDF

CMMC Model v1.02:

CMMC Model PDF

CMMC Model v1.02 Appendices:

CMMC Model Appendices PDF

CMMC Model v1.02 (Appendix A) in tabular format:

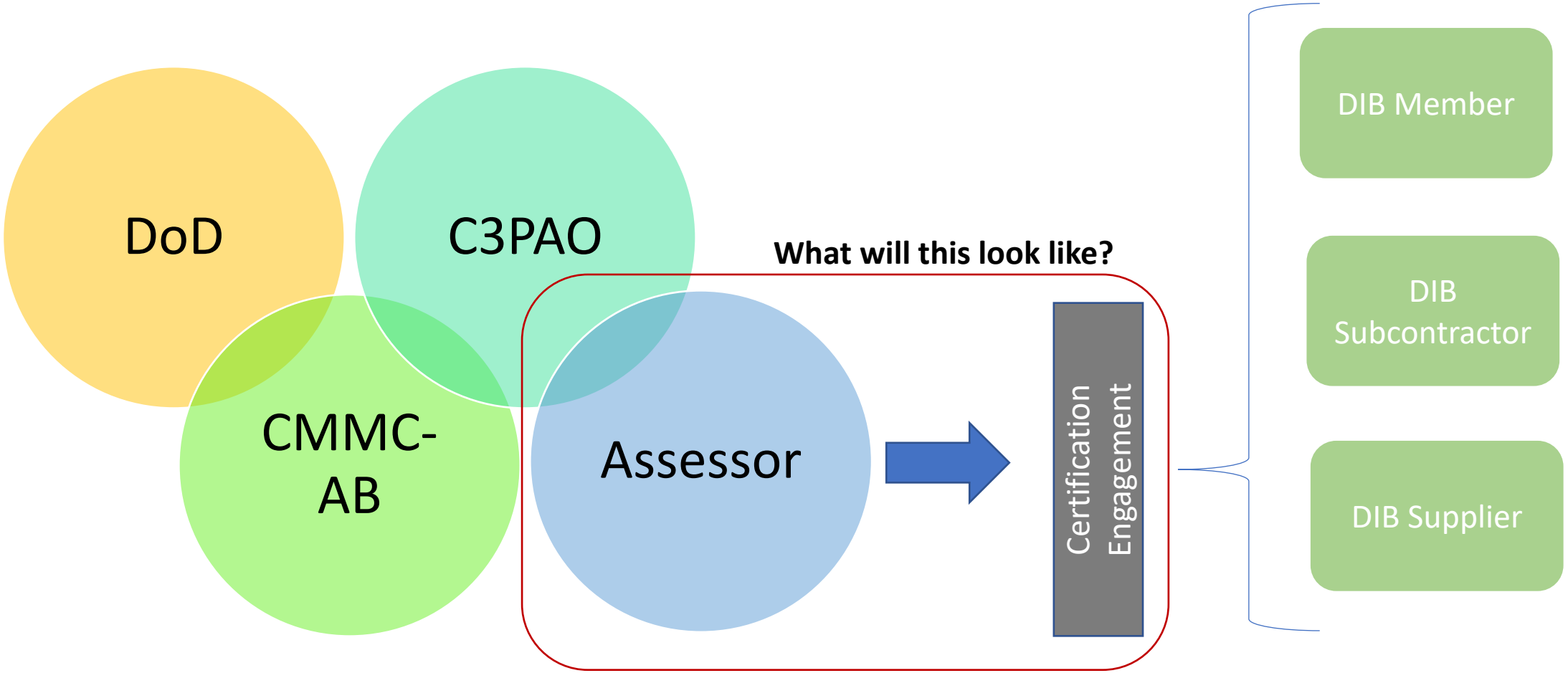
CMMC Model (Appendix A) Excel

CMMC Model Errata:

CMMC Model Errata PDF

https://www.acq.osd.mil/cmmc/draft.html - https://www.cmmcab.org/

Entities and Relationships



https://www.cmmcab.org/osc-lp

Comparison of Level 1 ⟷ Level 5

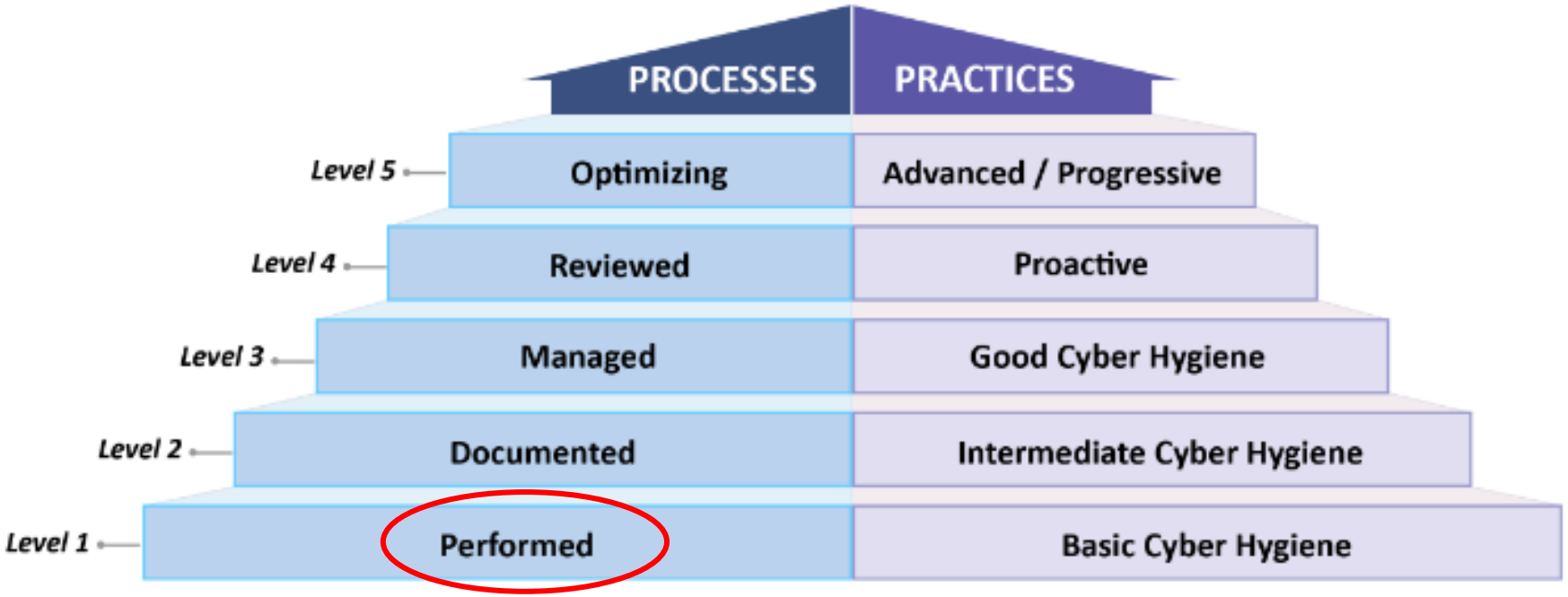
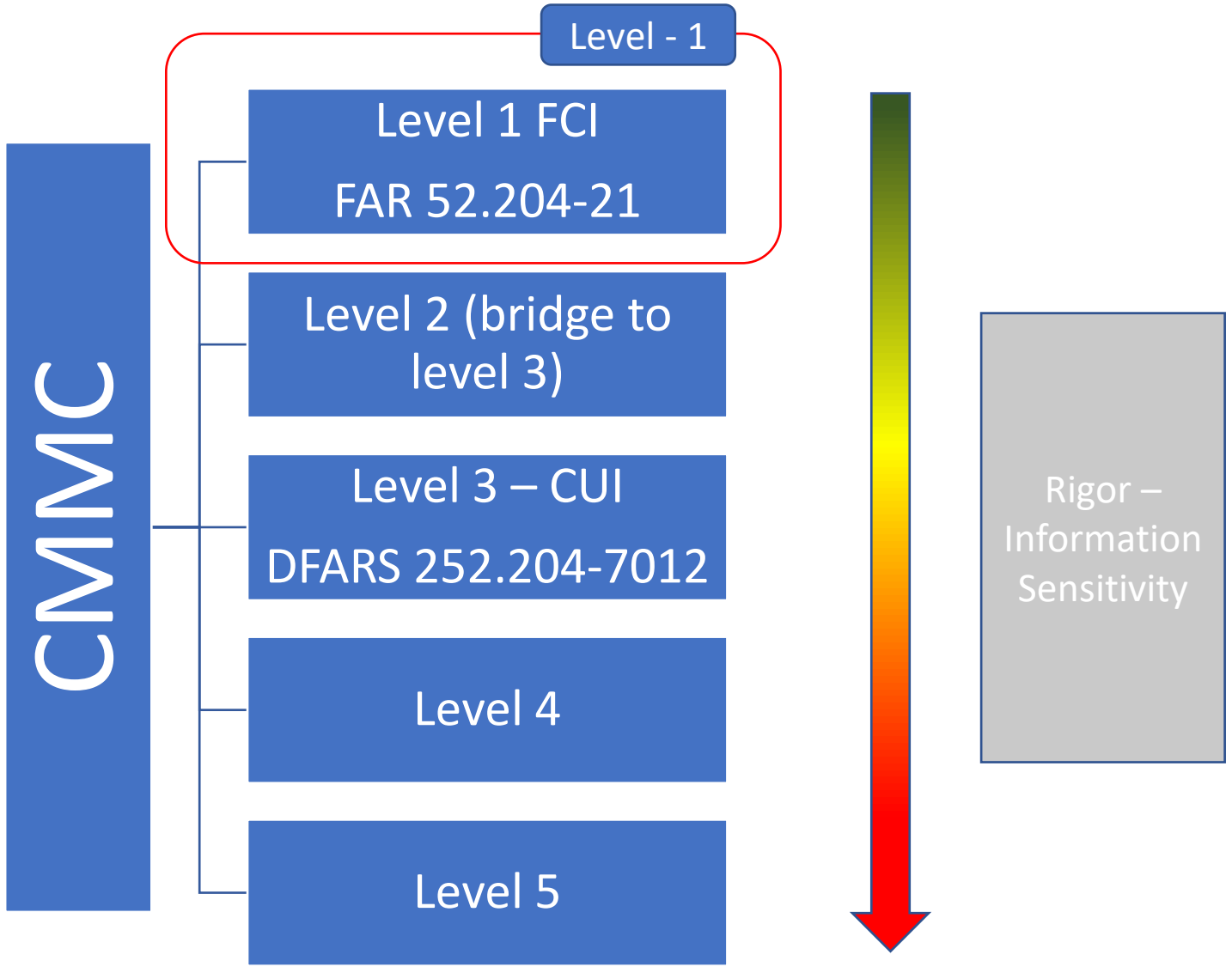


Figure 2. CMMC Levels and Descriptions

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


CMMC
Level - 1
Level 1 FCI
FAR 52.204-21
Level 2 (bridge to level 3)
Level 3 – CUI
DFARS 252.204-7012
Level 4
Level 5
Rigor – Information Sensitivity

CMMC – Levels overview

- Level 1:Safeguard Federal Contract Information (FCI)
- Level 2:Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3:Protect Controlled Unclassified Information (CUI)
- Levels 4-5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

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 Levels and Associated Focus

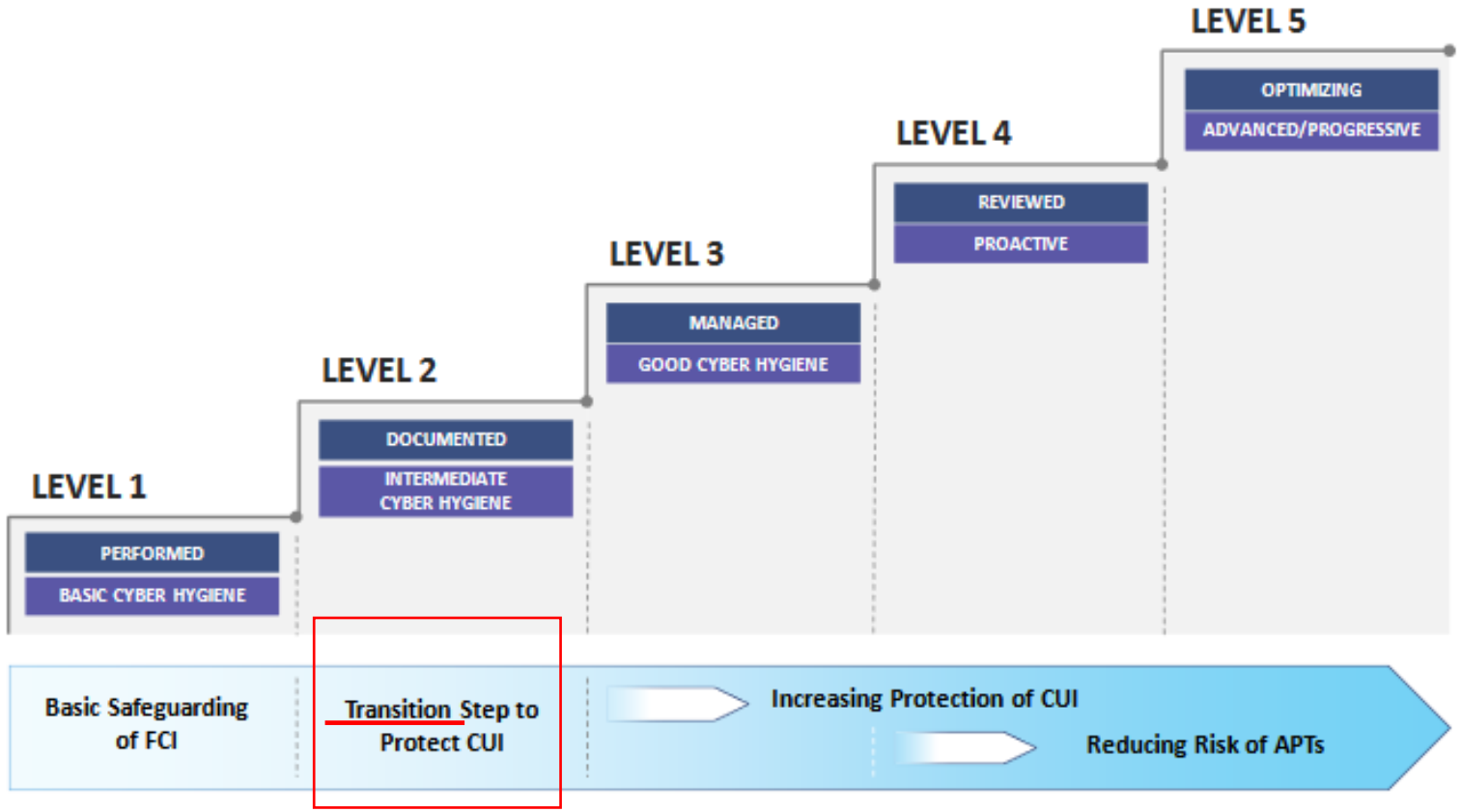
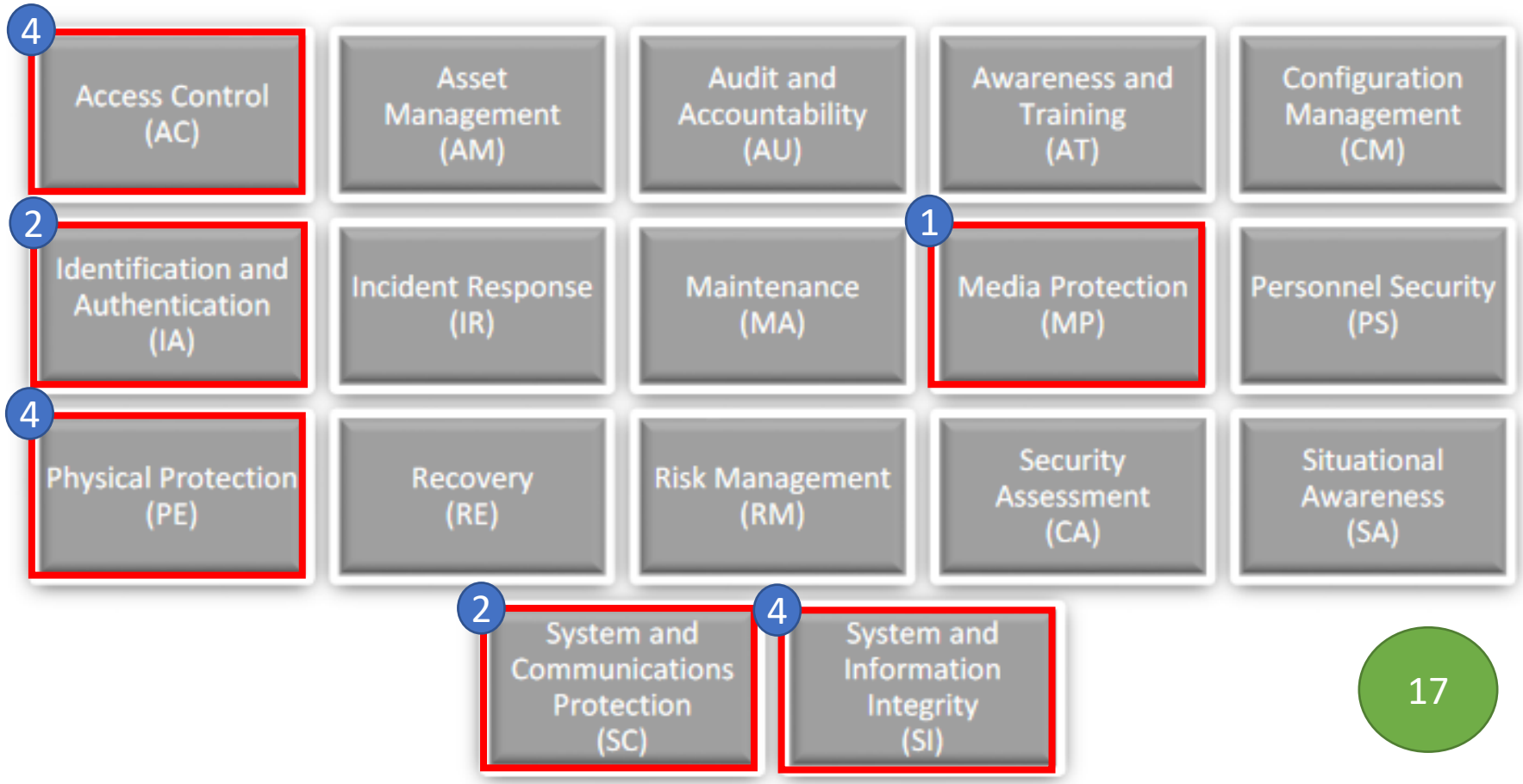


Figure 3. CMMC Levels and Associated Focus

CMMC - Domains

CMMC – Domains (Level-1)



Process Maturity Requirements

B.2.1 Process Maturity Level 1

There are currently no maturity processes at Level 1.

B.2.2 Process Maturity Level 2

ML.2.999: Establish a policy that includes [DOMAIN NAME].

DISCUSSION FROM SOURCE: CERT RMM V1.2

Develop and publish organizational policy for the process.

Establish the organizational expectations for planning and performing the process, and communicate these expectations via policy. The policy should reflect higher level managers' objectives for the process.

CMMC CLARIFICATION

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.

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

CMMC Level - 1

- Processes:

Performed Level 1 requires that an organization performs the specified practices. Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation, process maturity is not assessed for Level 1.

- Practices:

Basic Cyber Hygiene Level 1 focuses on the protection of FCI and consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 (“Basic Safeguarding of Covered Contractor Information Systems”) [3].

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

Key Definitions relative to CMMC Level 1

- Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release [3].
- Controlled Unclassified Information (CUI): CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended [4].

References

- Basic safeguarding requirements for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21
- Security requirements for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 [3, 4, 5].

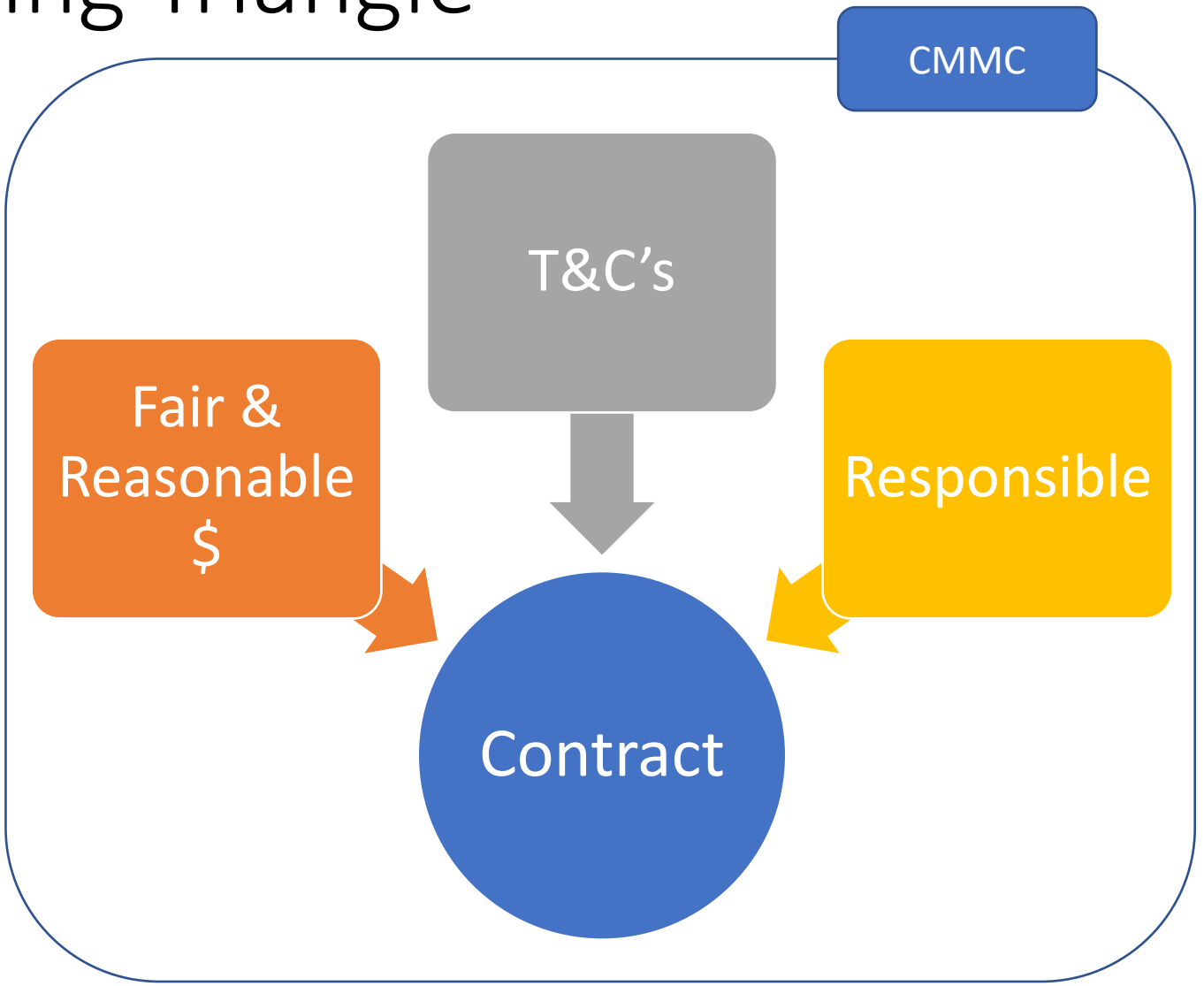
Considerations for Certification

- An official visitor contacts the company for the purpose of reviewing your cyber policies and procedures (CMMC).
- A meeting is set up.
- What do you provide this individual?
- What documentation should you be keeping and be able to provide?
- Should there be training records?
- How do these policies and procedures interface with other programs and requirements?
- How are these systems tested and/or exercised?

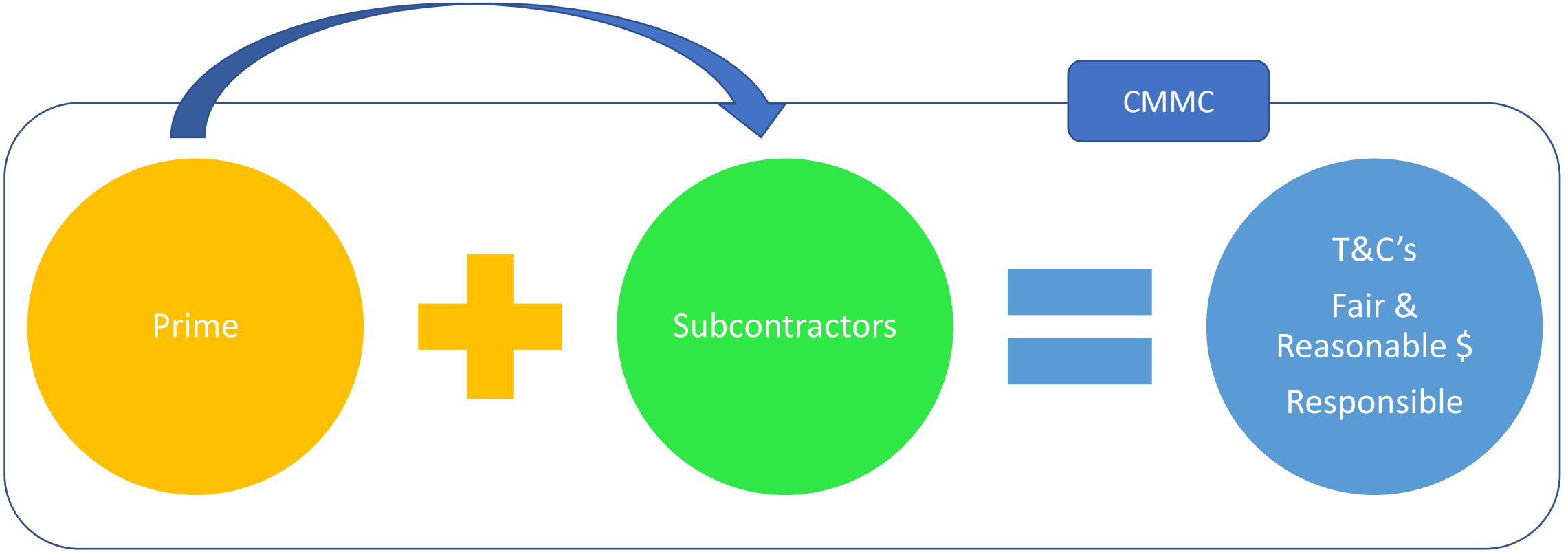
Critical Thinking – recurring theme

- Computer
- Network
- Voice – traditional/VOIP
- Web site
- Storage & Destruction
- Individuals
- Documents

Contracting Triangle

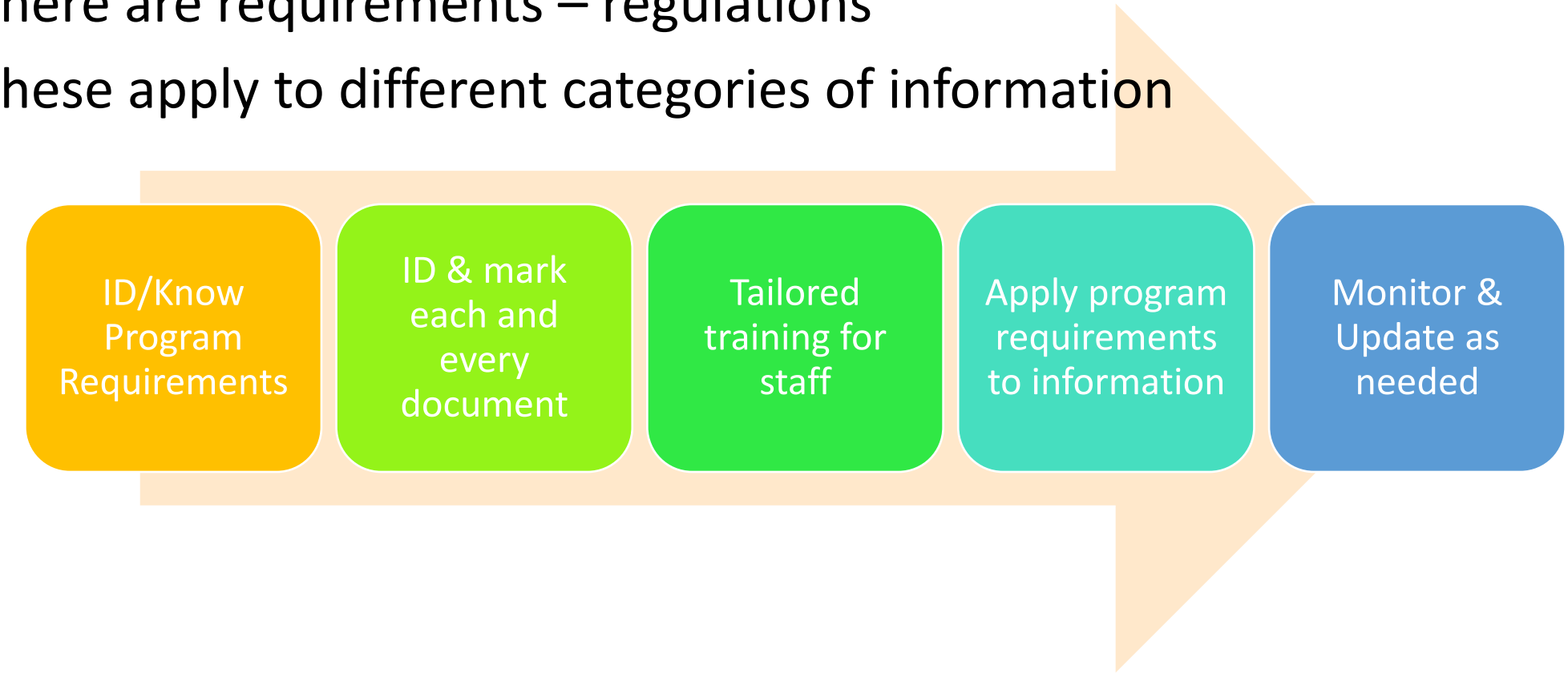


Contracting Equation

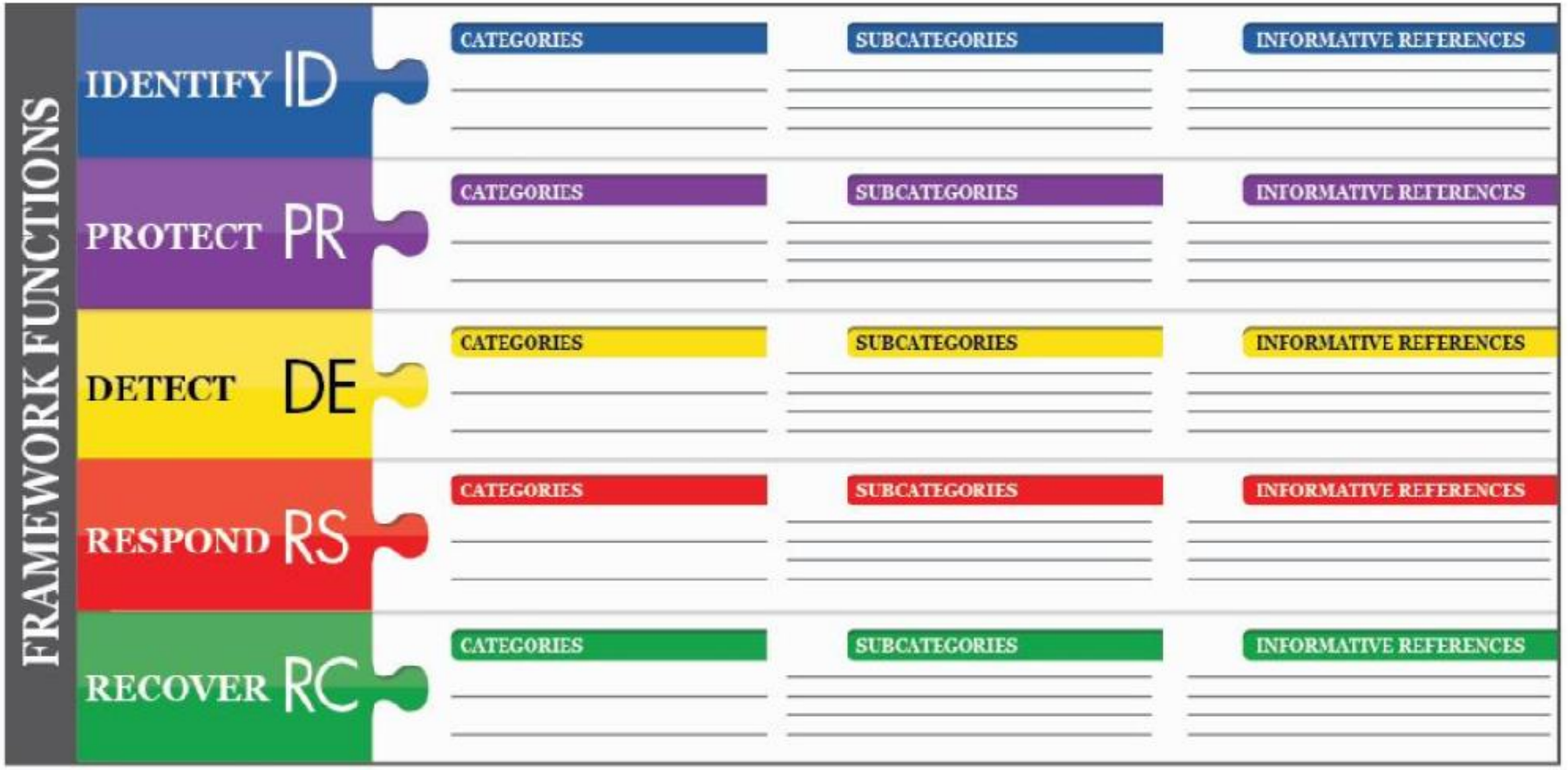


Commonalities

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



Cybersecurity Framework v1.1**



NIST CSF v1.1 PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 **CMMC L1 reference
Cybersecurity Framework v1.1 - https://doi.org/10.6028/NIST.CSWP.04162018 pg. 6

Cybersecurity Framework

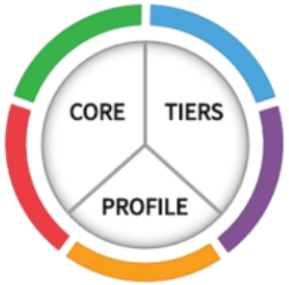
- **Framework** +
- **New to Framework** +
- **Perspectives** +
- **Success Stories** +
- **Online Learning** +
- **Evolution** +
- **Frequently Asked Questions** +
- **Events and Presentations** +
- **Related Efforts (Roadmap)**
- **Informative References** +
- **Resources** +
- **Newsroom** +
- **Related Programs**

CONNECT WITH US

Framework Version 1.1

The Cybersecurity Framework is ready to download.

Learn More



New to Framework

This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.

Learn More

Online Learning

Intro material for new Framework users to implementation guidance for more advanced Framework users.

Learn More

https://www.nist.gov/cyberframework

Cybersecurity Framework – key elements

- **Identify**–Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect**–Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect**–Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
- **Respond**–Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover**–Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due toa cybersecurity incident.

Framework for Improving Critical Infrastructure Cybersecurity; CSF v1.1, 2018; pg 7-8

CMMC elements

CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C001 Establish system access requirements	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	AC.2.005 Provide privacy and security notices consistent with applicable CUI rules. • NIST SP 800-171 Rev 1 3.1.9 • NIST SP 800-53 Rev 4 AC-8	

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

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

Familiarity with references can help

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

AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

DISCUSSION FROM SOURCE: DRAFT NIST SP 800-171 R2

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 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 (AC.1.002).

CMMC CLARIFICATION

Control who can use company computers and who can log on to the company network. Limit the services and devices, like printers, that can be accessed by company computers. Set up your system so that unauthorized users and devices cannot get on the company network.

Example 1

You are in charge of IT for your company. You give a username and password to every employee who uses a company computer for their job. No one can use a company computer without a username and a password. You give a username and password only to those employees you know have permission to be on the system. When an employee leaves the company, you disable their username and password immediately.

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf; page B-10

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** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	DISCUSSION 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** Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	ASSESSMENT OBJECTIVE *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 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]. Interview: [*SELECT FROM:* Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. 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

C001- Establish system access requirements – nb

- As companies seek to comply with CMMC — which features different standards depending on the nature of the work being done, with level 1 standards being the least demanding and level 5 the most burdensome — they should be aware of undetected devices on their networks that could pose risks to their certifications, said Katherine Gronberg, vice president of government affairs at Forescout Technologies, a San Jose, California-based security firm.

- "On average we can go into a company in any sector and find about 30 to 40 percent more devices than they knew about," she said.

https://www.nationaldefensemagazine.org/articles/2020/6/8/undetected-devices-may-pose-cmmc-issues

TM:SG4.SP1 –

Summary of Specific Goals and Practices

Goals	Practices
TM:SG1 Establish and Prioritize Technology Assets	TM:SG1.SP1 Prioritize Technology Assets
	TM:SG1.SP2 Establish Resilience-Focused Technology Assets
TM:SG2 Protect Technology Assets	TM:SG2.SP1 Assign Resilience Requirements to Technology Assets
	TM:SG2.SP2 Establish and Implement Controls
TM:SG3 Manage Technology Asset Risks	TM:SG3.SP1 Identify and Assess Technology Asset Risks
	TM:SG3.SP2 Address Technology Asset Risks
TM:SG4 Manage Technology Asset Integrity	TM:SG4.SP1 Control Access to Technology Assets
	TM:SG4.SP2 Perform Configuration Management
	TM:SG4.SP3 Perform Change Control and Management
	TM:SG4.SP4 Perform Release Management
TM:SG5 Manage Technology Asset Availability	TM:SG5.SP1 Perform Planning to Sustain Technology Assets
	TM:SG5.SP2 Manage Technology Asset Maintenance
	TM:SG5.SP3 Manage Technology Capacity
	TM:SG5.SP4 Manage Technology Interoperability

https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf TM | 2

TM:SG4.SP1 –

Technology assets are prioritized relative to their importance in supporting the delivery of high-value services.

The prioritization of technology assets must be performed in order to ensure that the organization properly directs its operational resilience resources to the assets that most directly impact and contribute to services that support the organization's mission. These assets require the organization's direct attention because their interruption or disruption has the potential to cause significant organizational consequences, particularly because the health and viability of information assets are typically tied directly to the resilience of technology assets.

Technology asset prioritization is performed relative to related services—that is, technology assets associated with high-value services are those that must be most highly prioritized for operational resilience activities. The organization may use other criteria to establish high-priority technology assets, such as

- the relationship between the technology and the value of the information assets stored, transported, or processed by the technology
- technology assets such as networks that are considered to be foundational and are vital to supporting more than one organizational service

Partial copy

https://resources.sei.cmu.edu/asset_files/Handbook/2016_002_001_514462.pdf TM | 3

C002 - Control internal system access

- AC.1.002
  Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
  - FAR Clause 52.204-21 b.1.ii
  - NIST SP 800-171 Rev 1 3.1.2
  - CIS Controls v7.1 1.4, 1.6, 5.1, 8.5, 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

C004 - Limit data access to authorized users and processes

- AC.1.003
  Verify and control/limit connections to and use of external information systems.
  - FAR Clause 52.204-21 b.1.iii
  - NIST SP 800-171 Rev 1 3.1.20
  - CIS Controls v7.1 12.1, 12.4
  - NIST CSF v1.1 ID.AM-4, PR.AC-3
  - CERT RMM v1.2 EXD:SG3.SP1
  - NIST SP 800-53 Rev 4 AC-20, AC-20(1)

C004 - Limit data access to authorized users and processes

- AC.1.004
  Control information posted or processed on publicly accessible information systems.
  - 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

C015 - Grant access to authenticated entities

- IA.1.076
  Identify information system users, processes acting on behalf of users, or devices.
  - FAR Clause 52.204-21 b.1.v
  - NIST SP 800-171 Rev 1 3.5.1
  - CIS Controls v7.1 4.2, 4.3, 16.8, 16.9
  - NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7
  - CERT RMM v1.2 ID:SG1.SP1
  - NIST SP 800-53 Rev 4 IA-2, IA-3, IA-5

C015 - Grant access to authenticated entities

- IA.1.077
  Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
  - FAR Clause 52.204-21 b.1.vi
  - NIST SP 800-171 Rev 1 3.5.2
  - CIS Controls v7.1 4.2, 4.3, 16.8, 16.9
  - NIST CSF v1.1 PR.AC-1, PR.AC-6, PR.AC-7
  - CERT RMM v1.2 TM:SG4.SP1
  - NIST SP 800-53 Rev 4 IA-2, IA-3, IA-5
  - UK NCSC Cyber Essentials

C024 - Sanitize media

- MP.1.118
  Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
  - FAR Clause 52.204-21 b.1.vii
  - NIST SP 800-171 Rev 1 3.8.3
  - NIST CSF v1.1 PR.DS-3
  - CERT RMM v1.2 KIM:SG4.SP3
  - NIST SP 800-53 Rev 4 MP-6

C028 - Limit physical access

- PE.1.131
  Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
  - FAR Clause 52.204-21 b.1.viii
  - NIST SP 800-171 Rev 1 3.10.1
  - NIST CSF v1.1 PR.AC-2
  - CERT RMM v1.2 KIM:SG4.SP2
  - NIST SP 800-53 Rev 4 PE-2

C028 - Limit physical access

- PE.1.133
  Maintain audit logs of physical access.
  - FAR Clause 52.204-21 Partial b.1.ix
  - NIST SP 800-171 Rev 1 3.10.4
  - NIST SP 800-53 Rev 4 PE-3

Look for wording that indicates documentation is/will be required.

C028 - Limit physical access

- PE.1.134
  Control and manage physical access devices.
  - FAR Clause 52.204-21 Partial b.1.ix
  - NIST SP 800-171 Rev 1 3.10.5
  - CERT RMM v1.2 KIM:SG4.SP2 – see next slide
  - NIST SP 800-53 Rev 4 PE-3

KIM:SG4 Manage Information Asset Confidentiality and Privacy

The confidentiality and privacy considerations of information assets are managed.

- Confidentiality and privacy are fundamental resilience requirements for information assets. These requirements are unique to information assets because the inadvertent or intentional disclosure of information to unauthorized staff can result in significant consequences to the organization, including reputation damage, harmful effects to customers and stakeholders (such as identity theft), and legal and financial penalties

C039 - Control communications at system boundaries

- SC.1.175
  Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
  - FAR Clause 52.204-21 b.1.x
  - NIST SP 800-171 Rev 1 3.13.1
  - NIST CSF v1.1 PR.PT-4
  - NIST SP 800-53 Rev 4 SC-7
  - UK NCSC Cyber Essentials

C039 - Control communications at system boundaries - a

System Boundary – All the components of an information system or an interconnected set of information resources under the same direct management control and security support structure, that share common functionality (normally includes hardware, software, information, data, applications, communications, and people).

Boundary Protection (or perimeter defense) – Tools and techniques used to manage, control and protect the security objectives of information stored, processed and transmitted within and between network boundaries; such as but not limited to controlled interfaces, intrusion detection, anti-virus, network forensic analysis, log monitoring.

Controlled Interfaces - Mechanisms that facilitate the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system such as but not limited to proxies, gateways, routers, firewalls, encrypted tunnels). https://gta-psg.georgia.gov/psg/network-security-boundary-protection-ss-08-047

Boundary protection is the "monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication." Protection is achieved through the use of gateways, routers, firewalls, guards, and encrypted tunnels.

https://insights.sei.cmu.edu/insider-threat/2018/09/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection.html

C039 - Control communications at system boundaries - a

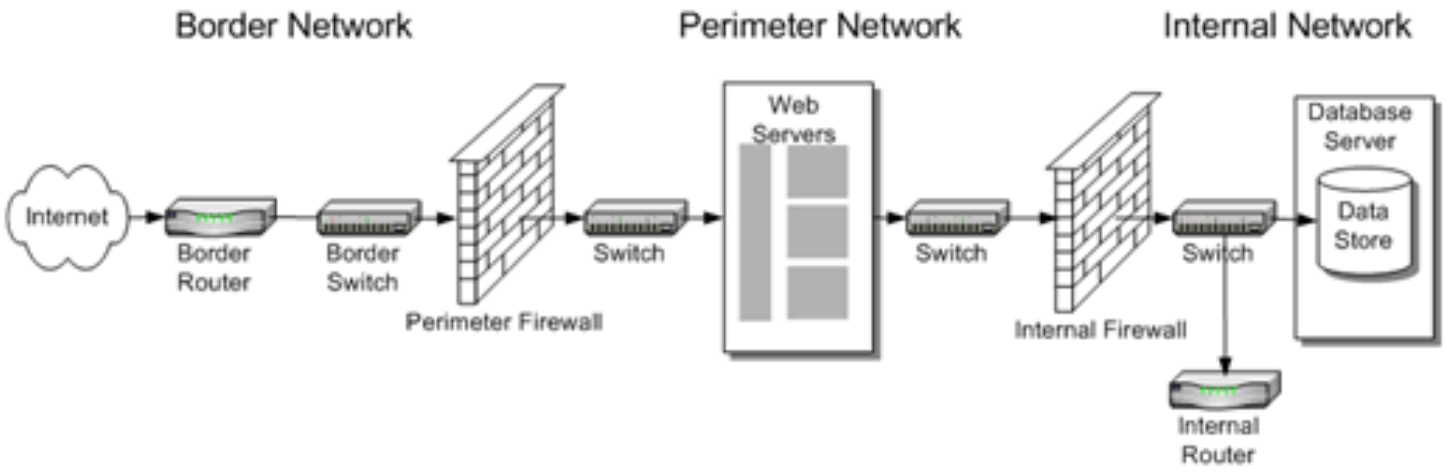


Figure 1. Enterprise Network Architecture

https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc700828(v=technet.10)?redirectedfrom=MSDN

C039Control communications at system boundaries

- SC.1.176
  Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
  - FAR Clause 52.204-21 b.1.xi
  - NIST SP 800-171 Rev 1 3.13.5
  - CIS Controls v7.1 14.1
  - NIST CSF v1.1 PR.AC-5
  - NIST SP 800-53 Rev 4 SC-7
  - UK NCSC Cyber Essentials

C040 - Identify and manage information system flaws

- SI.1.210
  Identify, report, and correct information and information system flaws in a timely manner.
  - FAR Clause 52.204-21 b.1.xii
  - NIST SP 800-171 Rev 1 3.14.1
  - NIST CSF v1.1 RS.CO-2, RS.MI-3
  - CERT RMM v1.2 VAR:SG2.SP2
  - NIST SP 800-53 Rev 4 SI-2
  - UK NCSC Cyber Essentials
  - AU ACSC Essential Eight

Should there be documentation?

C041 - Identify malicious content

- SI.1.211
  Provide protection from malicious code at appropriate locations within organizational information systems.
  - FAR Clause 52.204-21 b.1.xiii
  - NIST SP 800-171 Rev 1 3.14.2
  - CIS Controls v7.1 8.1
  - NIST CSF v1.1 DE.CM-4
  - CERT RMM v1.2 VAR:SG3.SP1
  - NIST SP 800-53 Rev 4 SI-3
  - AU ACSC Essential Eight

How would you show that this has been done? What defines appropriate locations?

C041 - Identify malicious content

- SI.1.212
  Update malicious code protection mechanisms when new releases are available.
  - FAR Clause 52.204-21 b.1.xiv
  - NIST SP 800-171 Rev 1 3.14.4
  - CIS Controls v7.1 8.2
  - NIST CSF v1.1 DE.CM-4
  - CERT RMM v1.2 VAR:SG3.SP1
  - NIST SP 800-53 Rev 4 SI-3

How do we track of?
How can it be shown that the protection is current as of a specific date?

C041 - Identify malicious content

- SI.1.213
  Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
  - FAR Clause 52.204-21 b.1.xv
  - NIST SP 800-171 Rev 1 3.14.5
  - CIS Controls v7.1 8.4, 8.7
  - NIST CSF v1.1 DE.CM-4
  - CERT RMM v1.2 VAR:SG3.SP1
  - NIST SP 800-53 Rev 4 SI-3

What, when, how, familiarity with/training & documentation

Suggestions – moving forward

- List all required elements
- Describe current position and/or processes
- Download/print all references for each requirement
- Compare
- Determine gaps
- Take internal/external actions to close gaps
- Identify resource – monitor
- Establish periodic review period

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

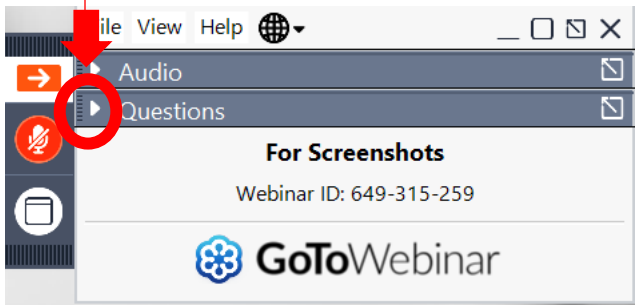
References - a

- https://ndisac.org/dibscc/implementation-and-assessment/top-10-high-value-controls/perimeter-hardening/

QUESTIONS?

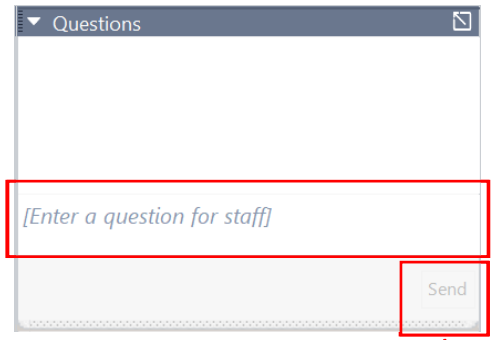
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

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

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINAR SERIES

- August 18, 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)

- August 26, 2020

  The Path to CMMC Level 3
  CLICK HERE for additional information
  Presented by Marc Violante, Wisconsin Procurement Institute

- September 15, 2020

  Analyzing and Responding to Federal Construction Solicitations
  CLICK HERE for additional information
  Presented by Helen Henningsen, Wisconsin Procurement Institute & Wenbin Yuan, Dakota Intertek Corp.

- September 30, 2020

  Government Property Management for Federal Contractors and Subcontractors
  CLICK HERE for additional information
  Presented by Ben Blanc, Wisconsin Procurement Institute

- October 21, 2020

  U.S. SBS Federal Women-Owned Small Business Program: The Transition is Happening Now
  CLICK HERE for additional information
  Presented by Kim Garber, Wisconsin Procurement Institute & Shane Mahaffy, US Small Business Administration (SBA)

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

…More at wispro.org/events

CYBER FRIDAY LIVE WEBINAR SERIES

Sept 11, 2020	A Deep Dive into DFARS 252.204-7012 - Looking beyond NIST 800-171 r1
Sept 25, 2020	Information Security - An overview of programs, general requirements and resources
Oct 9, 2020	Economic Espionage - You have what they want.
Oct 23, 2020	Guarding and Securing Intangibles - Protecting what you cannot see and touch
Nov 6, 2020	Tools, practices and resources for your cyber-security toolbox
Nov 20, 2020	An overview of cyber-threats - What you can't see - can put you out of business!
Dec 4, 2020	Securing the Supply Chain - "No man is an island"
Dec 18, 2020	Developing and implementing practices, policies and procedures using CMMC reference documents
Jan 8, 2021	The other side of CMMC
Jan 22, 2021	Overview of CMMC Level 1
Feb 5, 2021	Embarking on the path to CMMC Level 3
Feb 19, 2021	Preparing for a CMMC Certification assessment
Mar 5, 2021	CMMC Level 3 - Completing the steps needed to protect Controlled Unclassified Information.

PRESENTED BY

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

TECHNOLOGY INNOVATION CENTER at Research Park

NCMA National Contract Management Association
WISCONSIN

8/14/20

- SAVE THE DATE-

14th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In partnership with Volk Field ANG and Fort McCoy

October 15, 2020

<u>In-person</u> at Volk Field in Camp Douglas, WI

More info at wispro.org
https://www.wispro.org/event/14th-annual-wisconsin-government-business-opportunities-conference-gobc-2/

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

14th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In partnership with Volk Field ANG and Fort McCoy

HOSTS

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

worth a closer look
JUNEAU county

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

14th Annual Wisconsin Government Opportunities Business Conference (GOBC)

In partnership with Volk Field ANG and Fort McCoy

PARTNERS

WISCONSIN ECONOMIC DEVELOPMENT CORPORATION

AICCW FACC

BENTLEY

DUNN COUNTY ECONOMIC DEVELOPMENT CORPORATION

eNVISION GREATER FOND DU LAC

helping business grow Florence County Economic Development

INDIANHEAD COMMUNITY ACTION AGENCY, INC. OPENING DOORS. CREATING OPPORTUNITIES.

wdeoc WESTERN DAIRYLAND ECONOMIC OPPORTUNITY COUNCIL

NICOLET COLLEGE

NCMA NATIONAL CONTRACT MANAGEMENT ASSOCIATION WISCONSIN

NDIA Great Lakes

Northwest Regional Planning Commission NWRPC keeping your future as our focus

PROGRESS LAKESHORE Accelerating business success

UW-STOUT moc Manufacturing Outreach Center

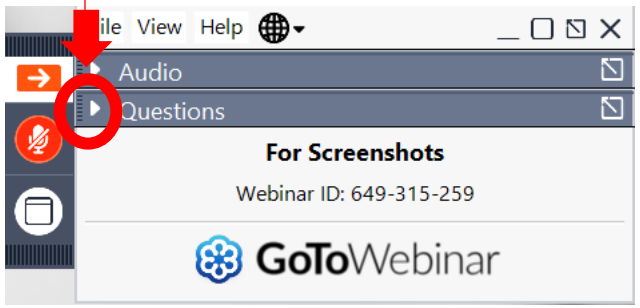
A CRITICAL NOTICE FROM WPI

- 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?

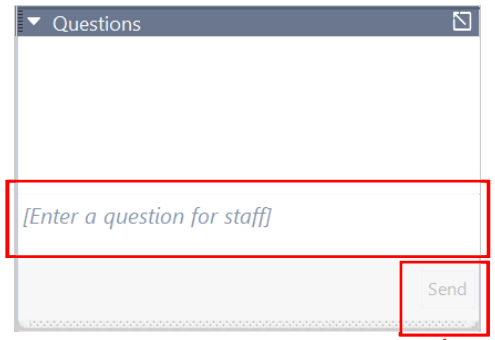
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

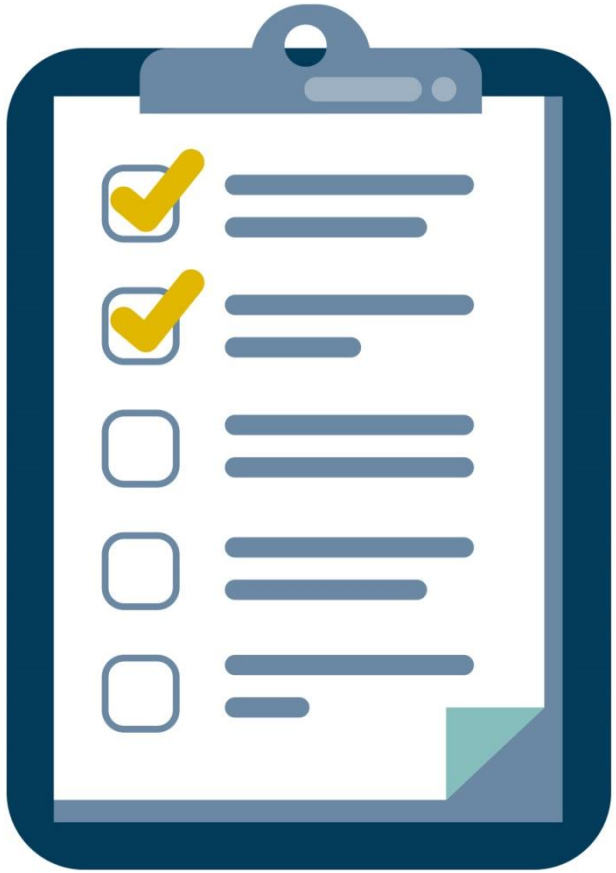
Type questions
here at any time
during a
presentation



Click Send when ready to submit a question

WPI 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 (WPI)
marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226