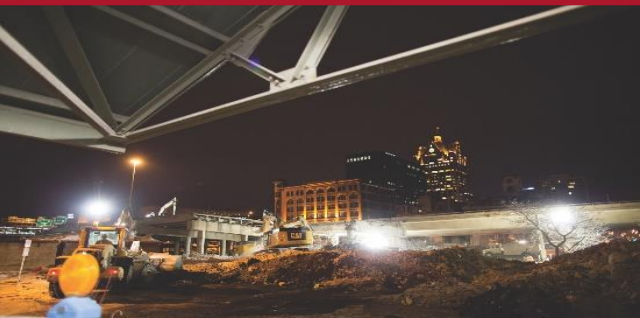


INTRODUCTION TO CMMC LEVEL 1 ACQUISITION HOUR WEBINAR

April 17, 2020



WEBINAR ETIQUETTE

PLEASE

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

THANK YOU!

ABOUT WPI SUPPORTING THE MISSION

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



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

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

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

WPI OFFICE LOCATIONS

▪ MILWAUKEE

- *Technology Innovation Center*

▪ MADISON

- *FEED Kitchens*
- *Dane County Latino Chamber of Commerce*
- *Wisconsin Manufacturing Extension Partnership (WMEP)*
- *Madison Area Technical College (MATC)*

▪ CAMP DOUGLAS

- *Juneau County Economic Development Corporation (JCEDC)*

▪ STEVENS POINT

- *IDEA Center*

▪ APPLETON

- *Fox Valley Technical College*

▪ OSHKOSH

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

▪ EAU CLAIRE

- *Western Dairyland*

▪ MENOMONIE

- *Dunn County Economic Development Corporation*

▪ LADYSMITH

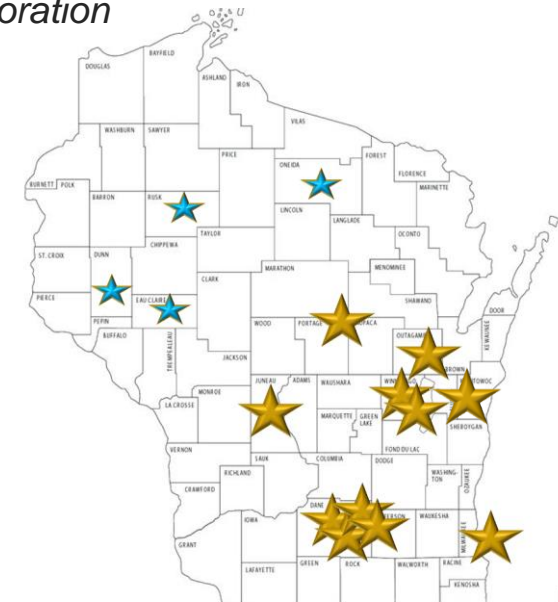
- *Indianhead Community Action Agency*

▪ RHINELANDER

- *Nicolet Area Technical College*

▪ GREEN BAY

- *Advance Business & Manufacturing Center*





Search ...

BLOG SERVICES ABOUT **CLIENT PORTAL** SPONSORSHIP CONTACT



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



www.wispro.org

UPCOMING EVENTS

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

[View More...](#)

CURRENT OPPORTUNITIES (1)

GET STARTED WITH THE BASICS

Questions & answers on how to get started.

[GET STARTED](#)

SIGN-UP FOR OUR NEWSLETTER

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

[SIGN UP](#)

HAVE A QUESTION? WE'RE HERE TO HELP.

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

[GET HELP](#)

Introduction to CMMC Level 1 requirements

Marc Violante

Wisconsin Procurement Institute

April 17, 2020

What we know - Current Cyber Obligations

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

Information Security Obligations/Requirements

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

What we don't know

- New DFARs (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.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

New DFARS

Open DFARS Cases as of April 03, 2020

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

CMMC Model v1.02 Release

- The Department is updating the documentation for CMMC Model v1.0 to correct administrative errors identified since January 31, 2020. The itemized list of corrected errata, as well as a more accessible version of the model (i.e. tabular format in Excel), are provided with the release of CMMC Model v1.02. The Department has made no substantive nor critical changes to the model relative to v1.0.

The Source!



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>

3/17/2020

Certification – resources/information



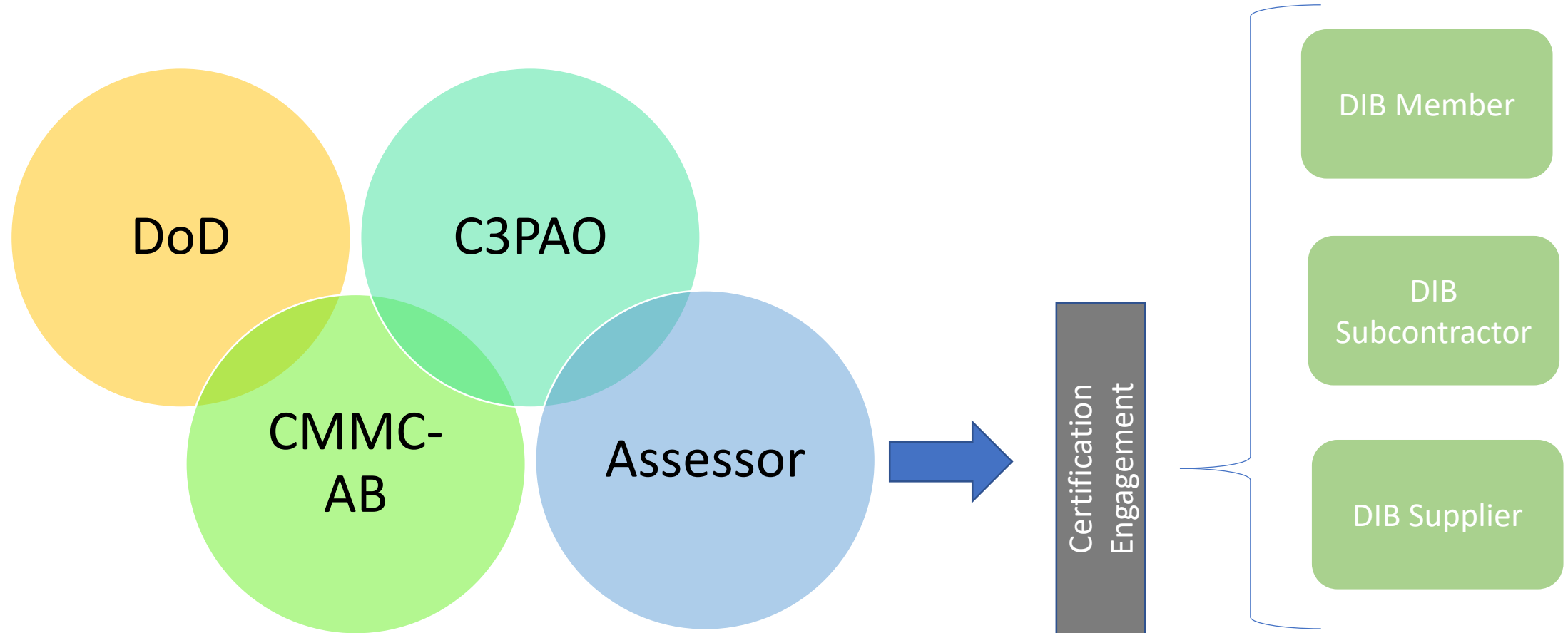
[Home](#) [CMMC Standard \(Official Page\)](#) [FAQ](#) [Glossary](#) [Stakeholders](#)
[Board of Directors](#) [Working Groups](#) [Speaking Engagements](#)

CMMC Accreditation Body (Cybersecurity Maturity Model Certification)

<https://www.cmmcab.org/>

3/17/2020

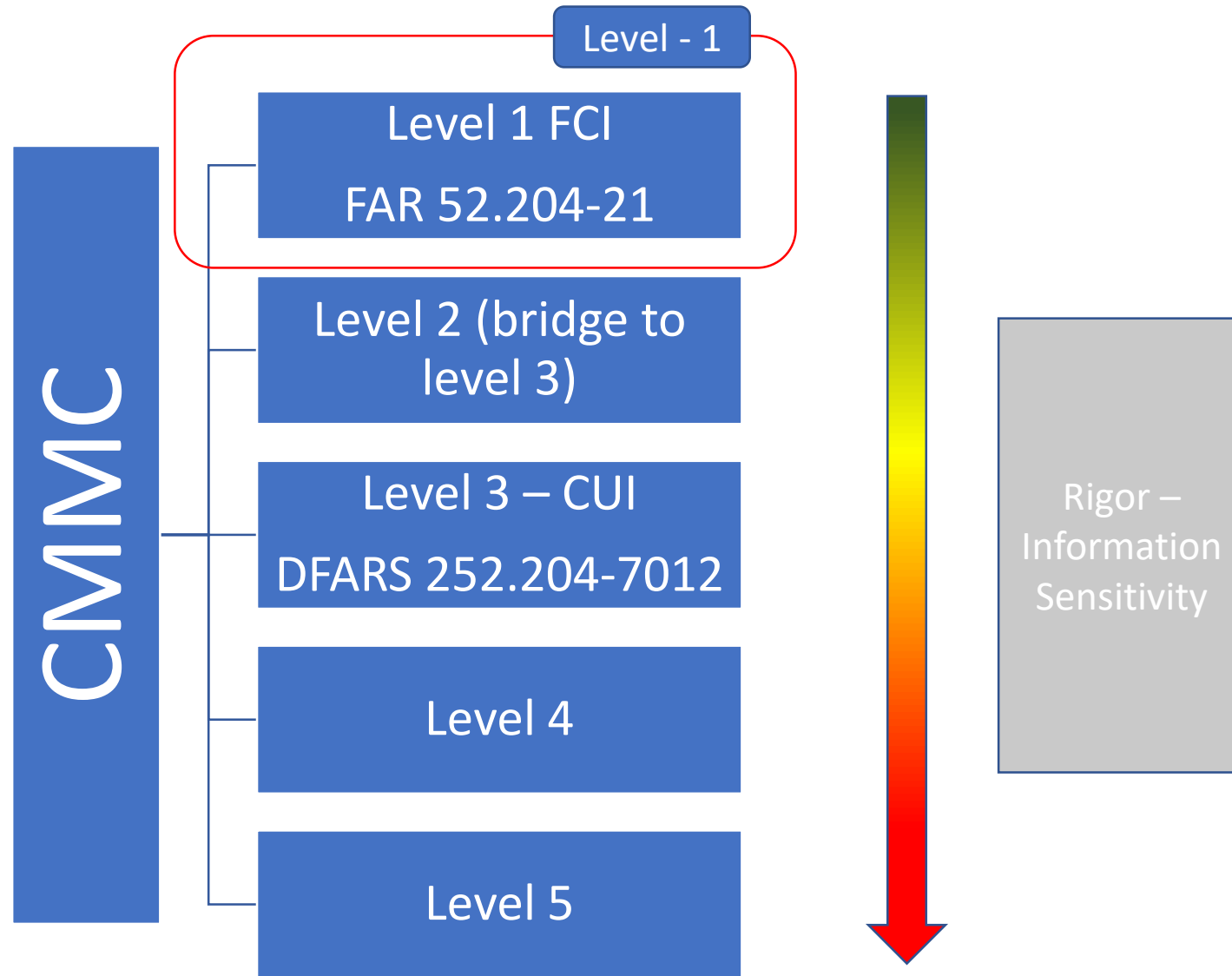
Entities and Relationships



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.

<https://www.acq.osd.mil/cmmc/updates.html>



Comparison of Level – 1 :: Level - 5

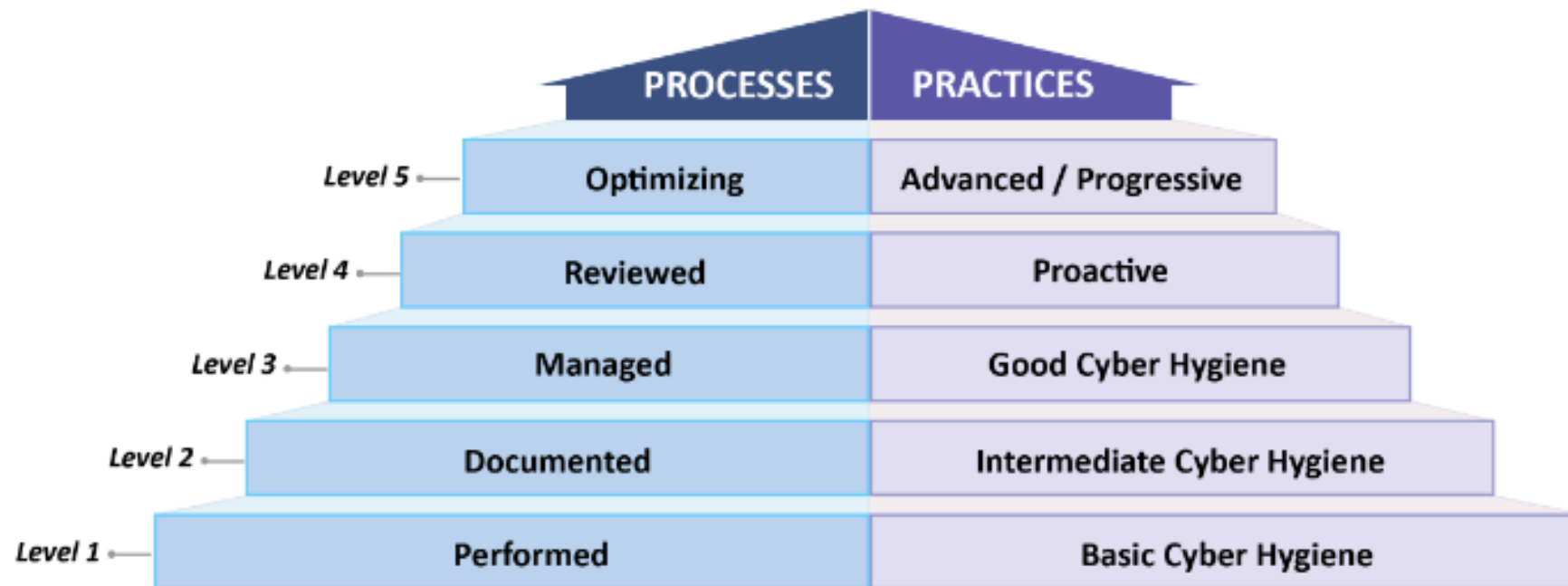


Figure 2. CMMC Levels and Descriptions

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

3/17/2020

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)

CMMC Levels and Associated Focus

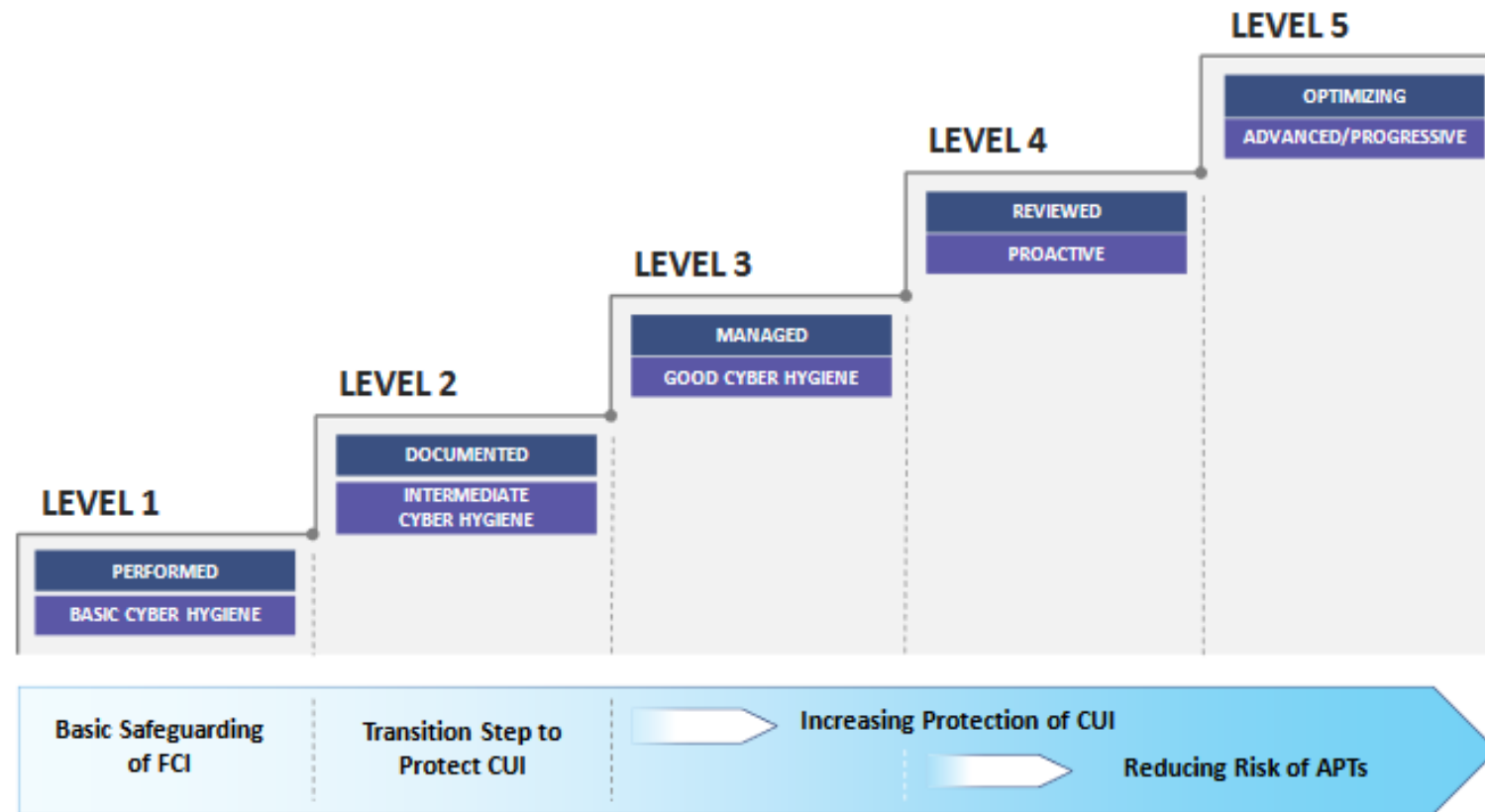


Figure 3. CMMC Levels and Associated Focus

3/17/2020

CMMC - Domains



Key Definitions relative to CMMC

- 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].

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].

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

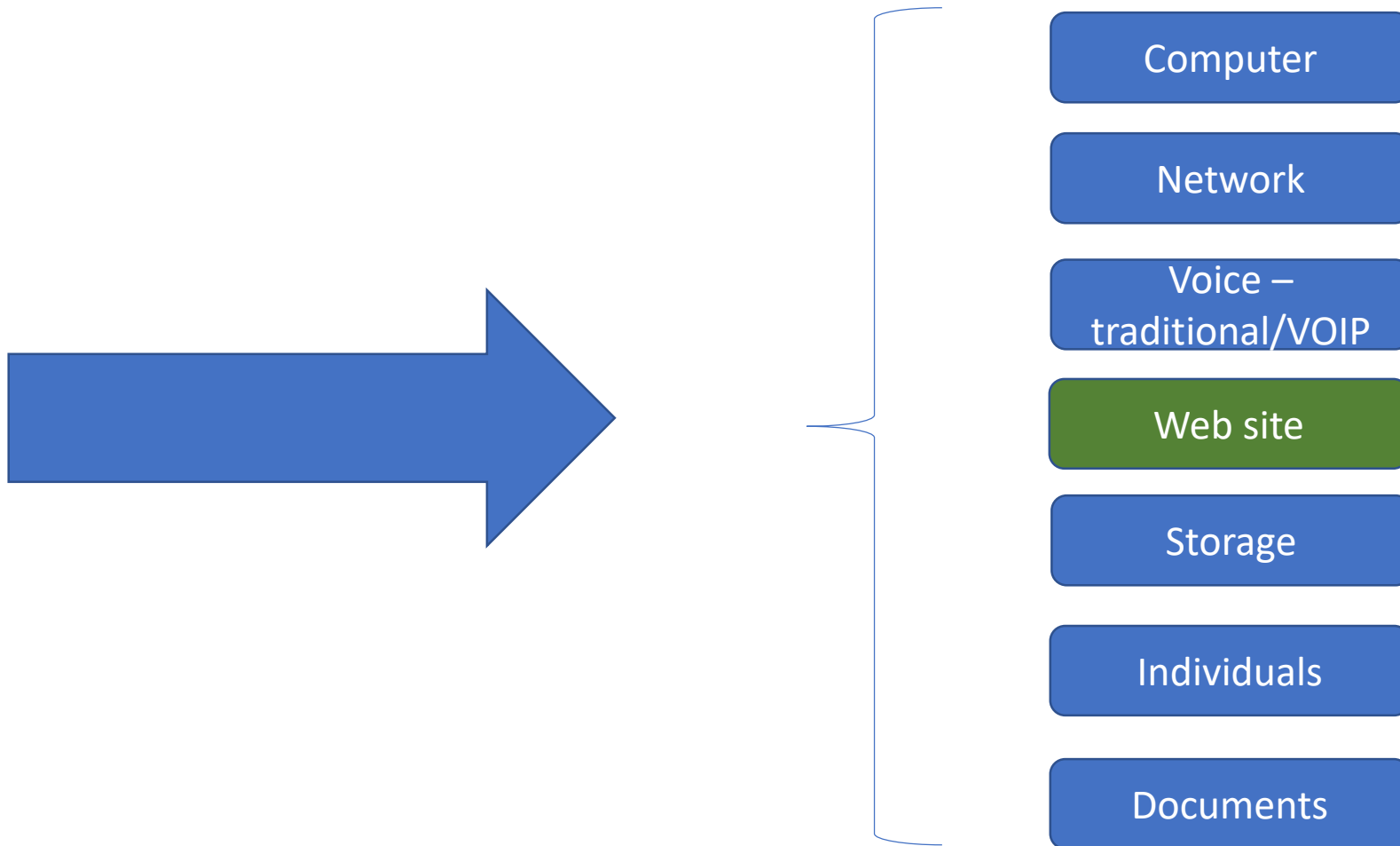
A policy is a high-level statement from an organization's senior management that documents the requirements for a given activity. It is intended to establish organizational expectations for planning and performing the activity, and communicate those expectations to the organization. Senior management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

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.

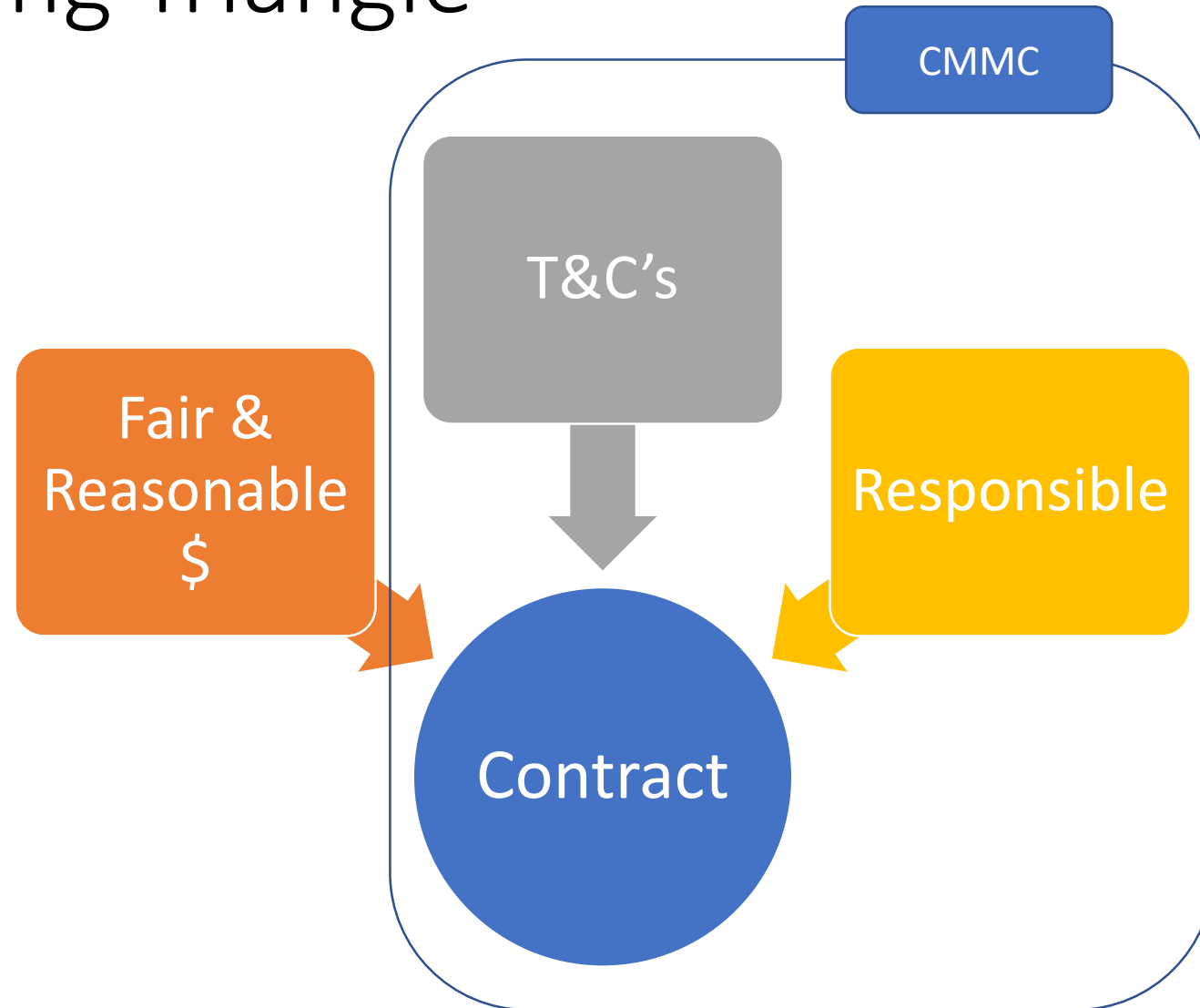
Critical Thinking – recurring theme



Information Security - today

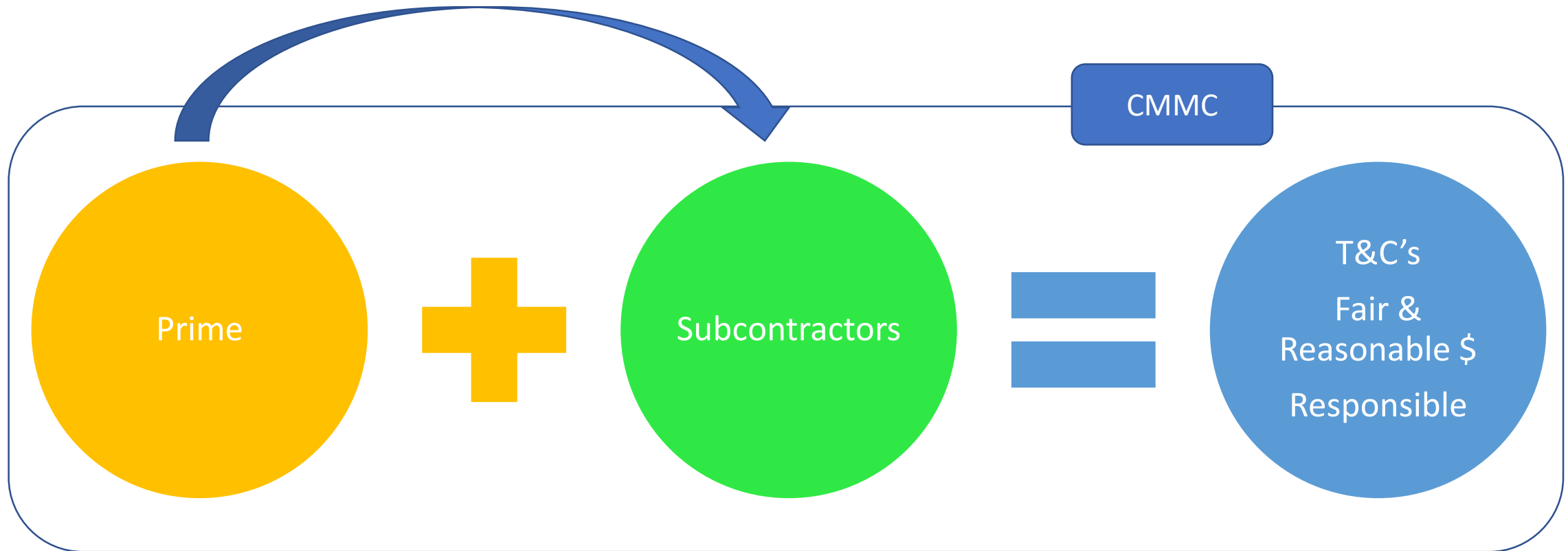
- Categories of information –
 - Federal Contract Information
 - Covered Defense Information = CTI & CUI
 - Controlled Unclassified Information
 - Impact Level
 - Export Controlled
 - JCP
 - ITAR
 - Other
 - Corporate – internal
 - Customer – contract/proprietary

Contracting Triangle



3/17/2020

Contracting Equation



Commonalities

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

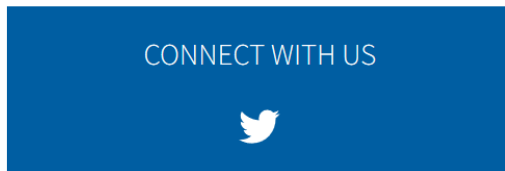


Cybersecurity Framework v1.1

FRAMEWORK FUNCTIONS	IDENTIFY ID	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	PROTECT PR	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	DETECT DE	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RESPOND RS	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES
	RECOVER RC	CATEGORIES	SUBCATEGORIES	INFORMATIVE REFERENCES

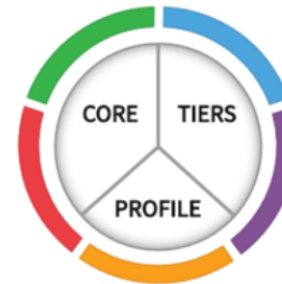
Cybersecurity Framework

- 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**



Framework Version 1.1

The Cybersecurity Framework is ready to download.



New to Framework

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



Online Learning

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



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 to a cybersecurity incident.

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

3/17/2020

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?

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

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.

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.1.132
Escort visitors and monitor visitor activity.
 - FAR Clause 52.204-21 Partial b.1.ix
 - NIST SP 800-171 Rev 1 3.10.3
 - CERT RMM v1.2 AM:SG1.SP1
 - NIST SP 800-53 Rev 4 PE-3

Limit physical access PE.1.132

- FAR 52.204-21
 - (ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
- NIST 800-171 r1
 - 3.10.3 Escort visitors and monitor visitor activity.
 - DISCUSSION Individuals with permanent physical access authorization credentials are not considered visitors. Audit logs can be used to monitor visitor activity.

Limit physical access PE.1.132

AM:SG1.SP1 Enable Access

- Appropriate access to organizational assets is established based on resilience requirements and appropriate approvals.
 - Access privileges and restrictions describe the level and extent of access provided to identities. Access privileges should be commensurate with the various roles represented by an identity but concurrently must be congruent with the resilience requirements of the assets to which the privileges are granted. Access privileges are assigned and approved by asset owners based on the role of the person, object, or entity that is requesting access. Asset owners are the persons or organizational units, internal or external to the organization, that have primary responsibility for the viability, productivity, and resilience of a high-value organizational asset. It is the owner's responsibility to ensure that requirements for protecting and sustaining assets are defined for assets under the owner's control.

Limit physical access PE.1.132

Partial copy

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

- a. Enforces physical access authorizations at [*Assignment: organization-defined entry/exit points to the facility where the information system resides*] by;
 1. Verifying individual access authorizations before granting access to the facility; and
 2. Controlling ingress/egress to the facility using [*Selection (one or more): [Assignment: organization-defined physical access control systems/devices]; guards*];
- b. Maintains physical access audit logs for [*Assignment: organization-defined entry/exit points*];
- c. Provides [*Assignment: organization-defined security safeguards*] to control access to areas within the facility officially designated as publicly accessible;
- d. Escorts visitors and monitors visitor activity [*Assignment: organization-defined circumstances requiring visitor escorts and monitoring*];
- e. Secures keys, combinations, and other physical access devices;
- f. Inventories [*Assignment: organization-defined physical access devices*] every [*Assignment: organization-defined frequency*]; and

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

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
 - 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

- 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

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

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

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

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>

UPCOMING TRAINING - EVENTS

ACQUISITION HOUR LIVE WEBINARS SERIES

▪ April 17, 2020

Intro to CMMC Level 1

[CLICK HERE](#) for additional information

Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

▪ April 22, 2020

Packaging, Shipping and Invoicing Using WAWF and PIEE

[CLICK HERE](#) for additional information

Presented by Lisa Dixon & John Hoeffler, Bentley World Packaging

▪ April 21, 2020

How to Quickly Analyze Solicitations

[CLICK HERE](#) for additional information

Presented by Helen Henningsen, Wisconsin Procurement Institute (WPI)

▪ April 23, 2020

The Emergency Paid Sick Leave Act & The Emergency Family & Medical Leave Expansion Act – The Basics

[CLICK HERE](#) for additional information

Presented by Corey Walton, DOL

ACQUISITION HOUR LIVE WEBINARS SERIES

▪ April 24, 2020

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

[CLICK HERE](#) for additional information
Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

▪ April 29, 2020

Economic Espionage – Awareness of Threats & Resources for Gov't Contractors

[CLICK HERE](#) for additional information
Presented by Marc Violante, Wisconsin Procurement Institute (WPI)

▪ May 5, 2020

Learning About the Surety Bond Guarantee from the US SBA

[CLICK HERE](#) for additional information
Presented by the US Small Business Administration

▪ May 19, 2020

Pieces of the Proposal Puzzle

[CLICK HERE](#) for additional information
Presented by Helen Heningsen, Wisconsin Procurement Institute (WPI)

...More at wispro.org/events

14TH ANNUAL WISCONSIN GOVERNMENT BUSINESS OPPORTUNITIES CONFERENCE (GOBC)

June 24 - June 25

Details

Start:
June 24

End:
June 25

Event Categories:
Conference, WPI Events

Organizer

Hilary DeBlois

Phone:
(414) 688-3882

Email:
hilaryd@wispro.org

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

Venue

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



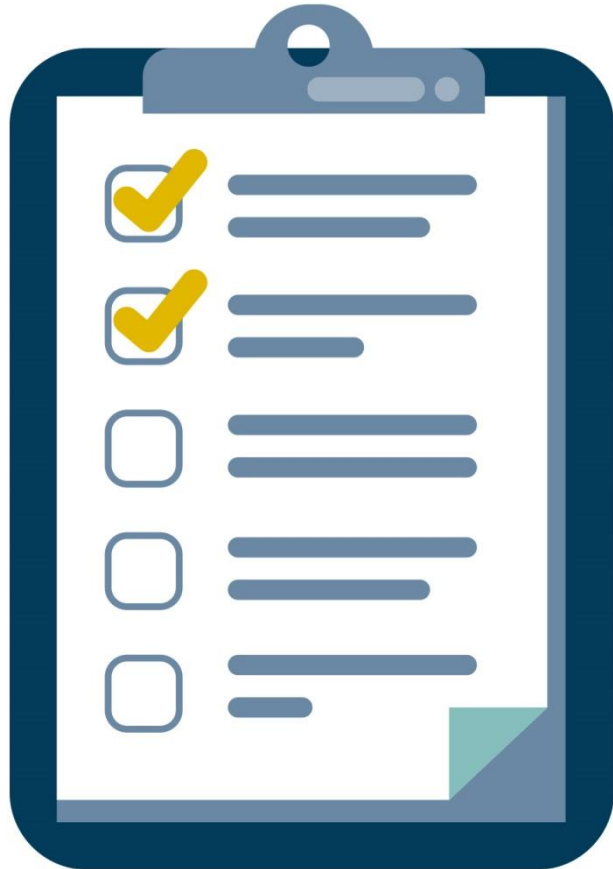
A CRITICAL NOTICE FROM WPI

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

QUESTIONS?



SURVEY



CONTINUING PROFESSIONAL EDUCATION



CPE Certificate available, please contact:

Benjamin Blanc

benjaminb@wispro.org

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Marc Violante, Wisconsin Procurement Institute

marcv@wispro.org | 920-456-9990

10437 Innovation Drive, Suite 320
Milwaukee, WI 53226