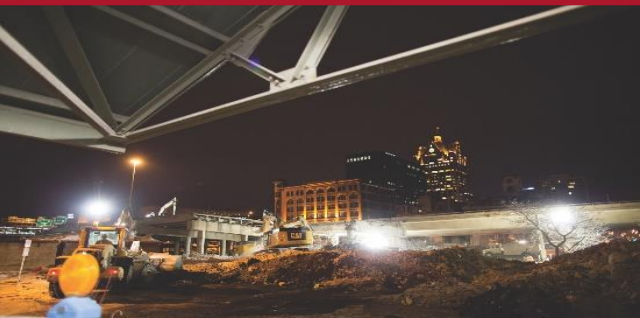


INTRODUCTION TO CMMC LEVEL 1

ACQUISITION HOUR WEBINAR

June 12, 2020



WEBINAR ETIQUETTE

PLEASE

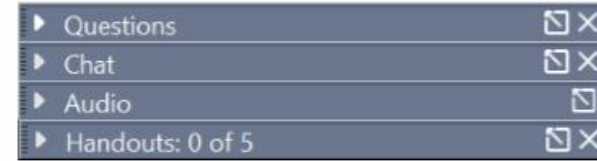
- Log into the GoToWebinar session with the name that you registered with online
- Place your phone or computer on MUTE
- Use the QUESTIONS option to ask your question(s).
 - We will share the questions with our guest speaker who will respond to the group

THANK YOU!

GoToWebinar Control Panel



In-Session Tools

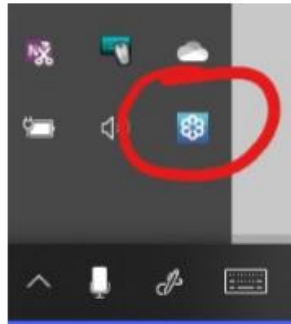


Audio Problems?

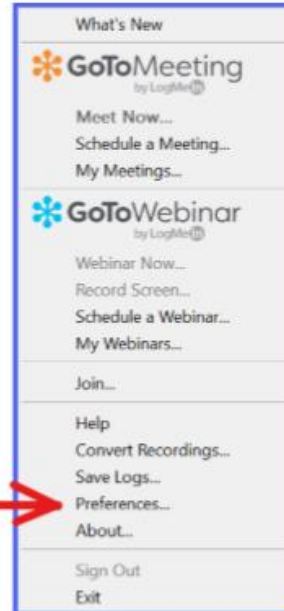
1



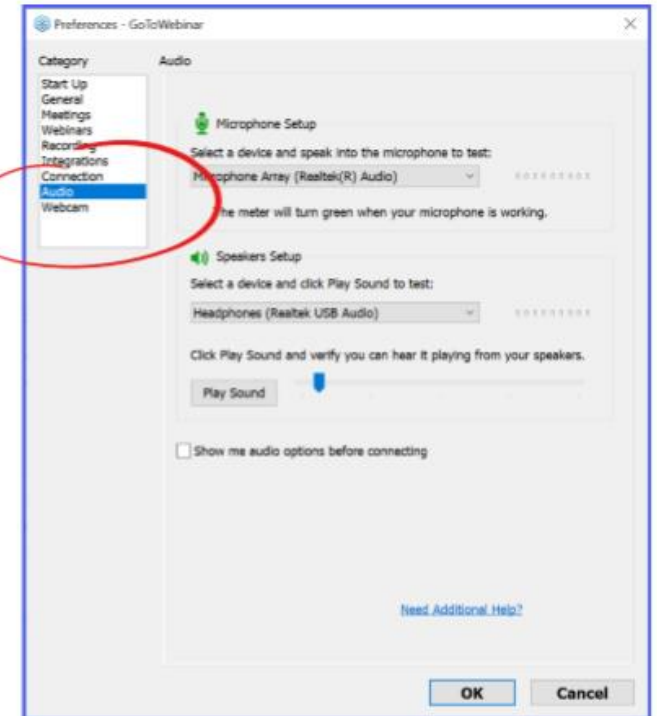
2



3



4



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

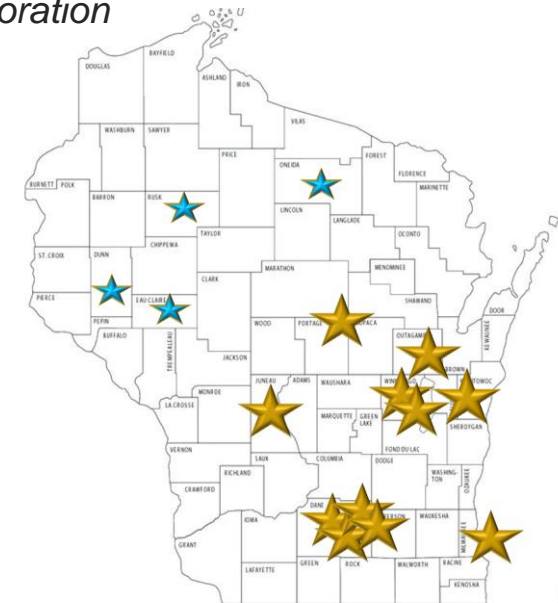
- *Indianhead Community Action Agency*

▪ RHINELANDER

- *Nicolet Area Technical College*

▪ GREEN BAY

- *Advance Business & Manufacturing Center*





Search ...

BLOG SERVICES ABOUT **CLIENT PORTAL** SPONSORSHIP CONTACT



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

CURRENT EDITION OF THE WPI NEWSLETTER

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

June 12, 2020

Today's goals

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

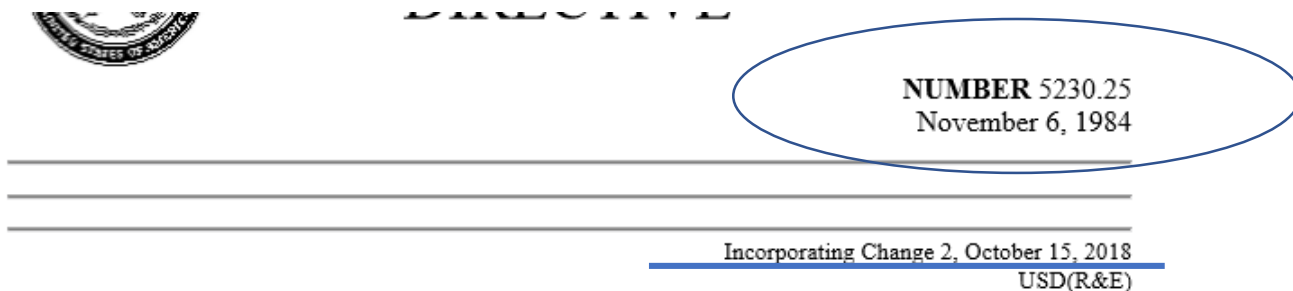
What we know - Current Cyber Obligations

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
- DON – Geurts memos – CDRL requirements
- Other requirements

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

Reference – DD Form 2345 - JCP



REFERENCES, continued

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

- (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**.

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

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

6/12/2020



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



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/>

6/12/2020

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

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/>

6/12/2020

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!

Information is a powerful driver!

The screenshot shows the homepage of Successful Farming at Agriculture.com. The top navigation bar includes links for Talk, Magazine, TV, Radio, Login, Join, and Newsletter, along with a search box. The main navigation menu lists categories: NEWS, MARKETS, WEATHER, MACHINERY, CROPS, TECHNOLOGY, FARM MANAGEMENT, LIVESTOCK, and FAMILY. A dropdown menu for 'MARKETS' is open, showing options: Commodity Prices, Newswire, Markets Analysis, and Your World in Agriculture. On the left sidebar, there are sections for 'TALK IN MA' with a sub-section 'Blue Sky 2017' and 'Floor Talk November 7'. The main content area features a breadcrumb trail 'Home > News > Business' and a large red headline: 'CHINESE NATIONALS CHARGED WITH STEALING CORN TECHNOLOGY'. Below the headline, it says 'By Jeff Caldwell' and '12/13/2013'.

6/12/2020

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>

6/12/2020

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.

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

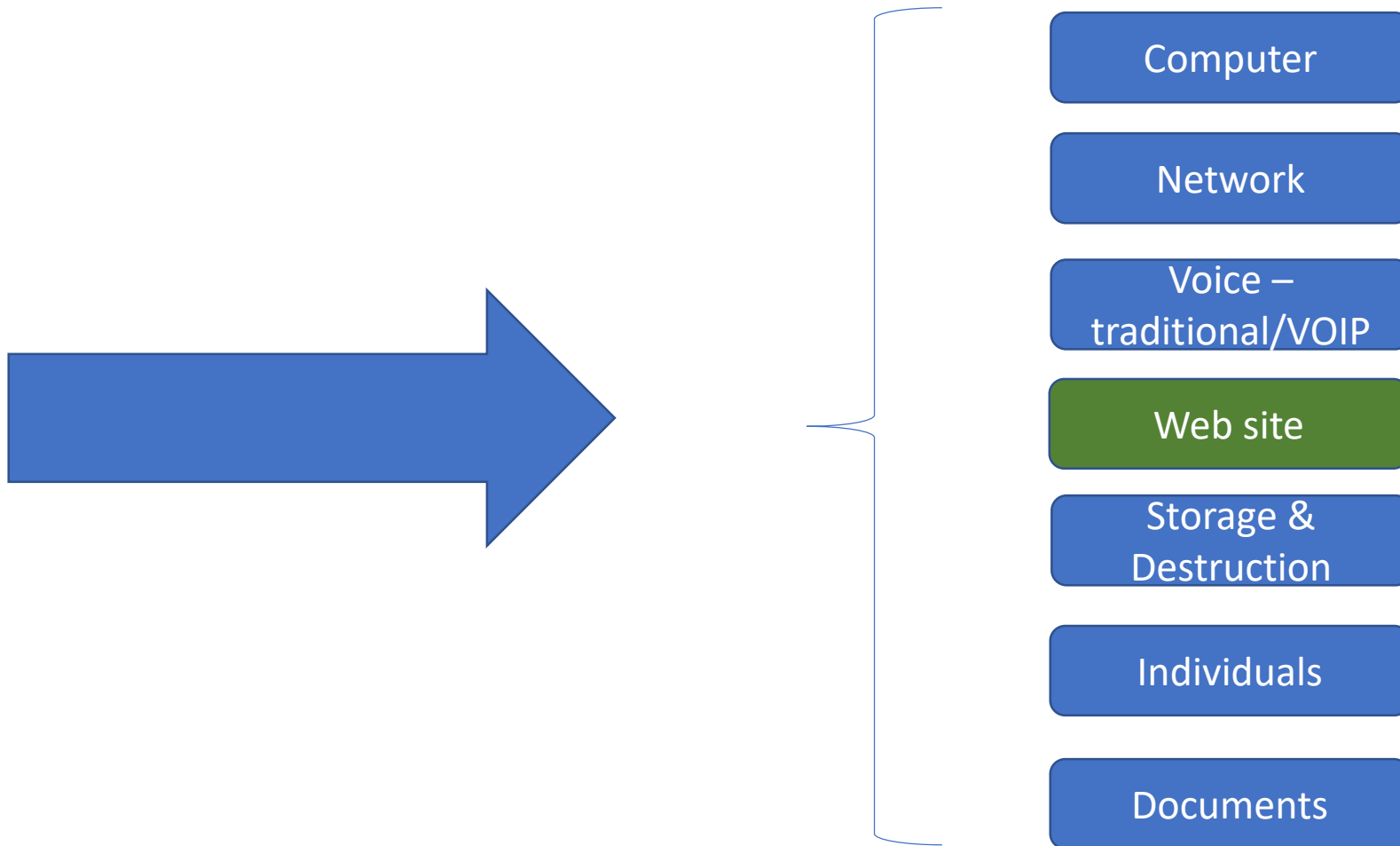
*Level 1 does not specify documentation but...?

New DFARS -

Open DFARS Cases as of June 08, 2020

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.
-----------	---	--	---

Critical Thinking – recurring theme



6/12/2020

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.

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/>

6/3/2020

Certification – resources/information



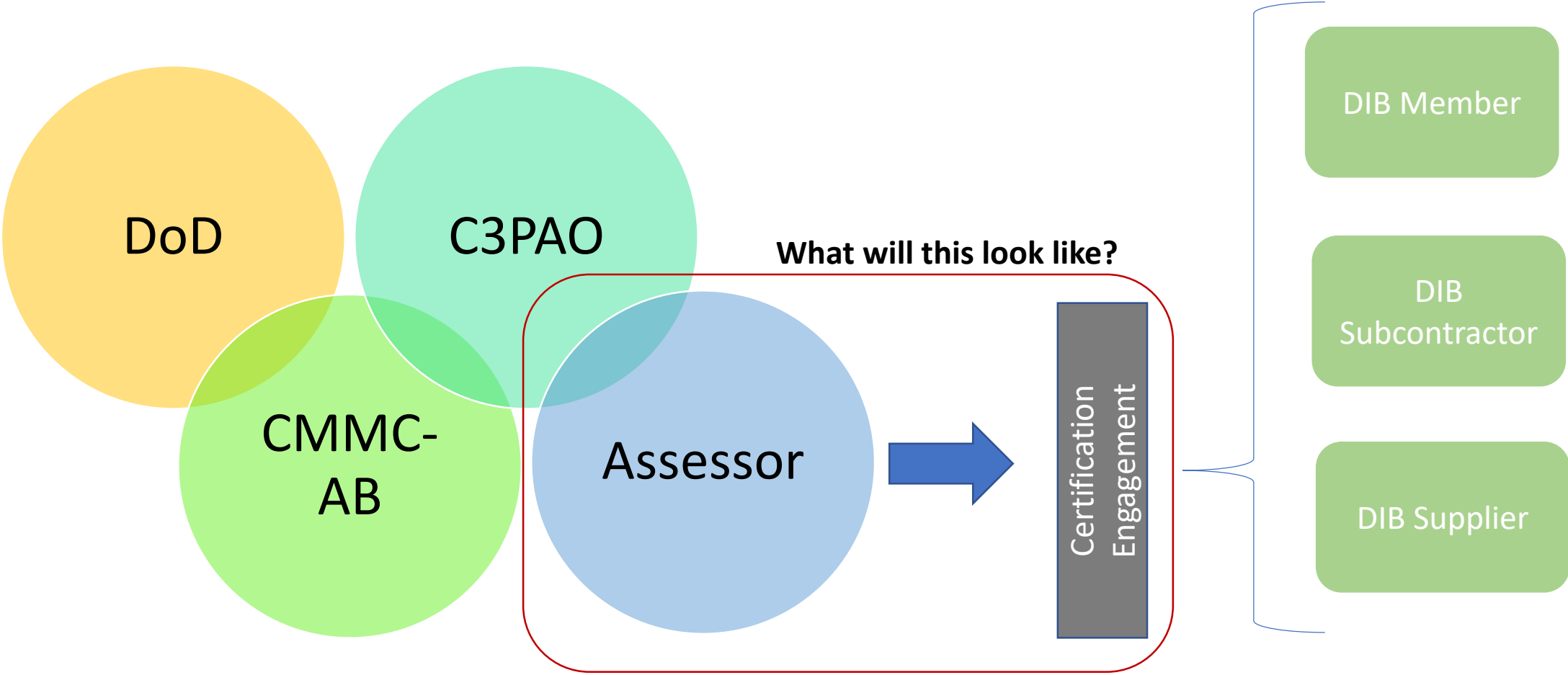
[Home](#) [CMMC Standard \(Official Page\)](#) [FAQ](#) [Glossary](#) [Stakeholders](#)
[Board of Directors](#) [Working Groups](#) [Speaking Engagements](#)

CMMC Accreditation Body (Cybersecurity Maturity Model Certification)

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

6/12/2020

Entities and Relationships



CMMC Model v1.02 Release (evolving)

- 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>

6/12/2020

Comparison of Level 1 ↔ Level 5

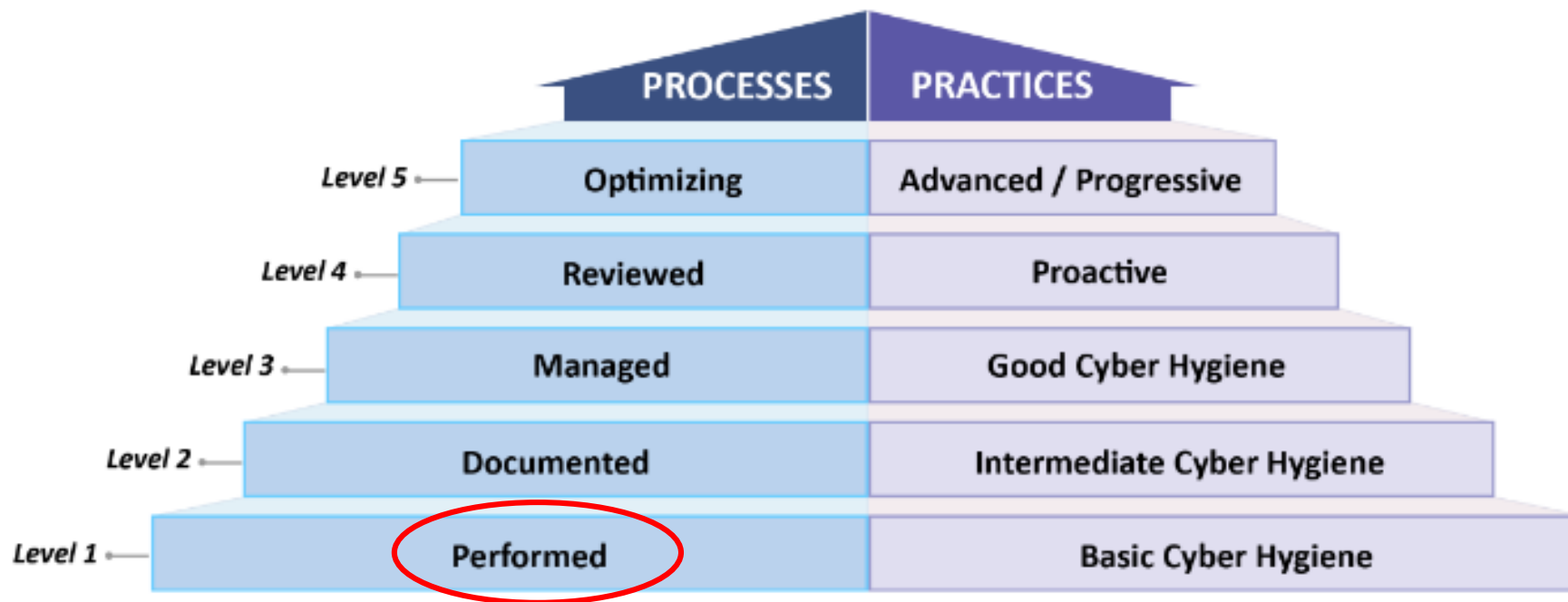
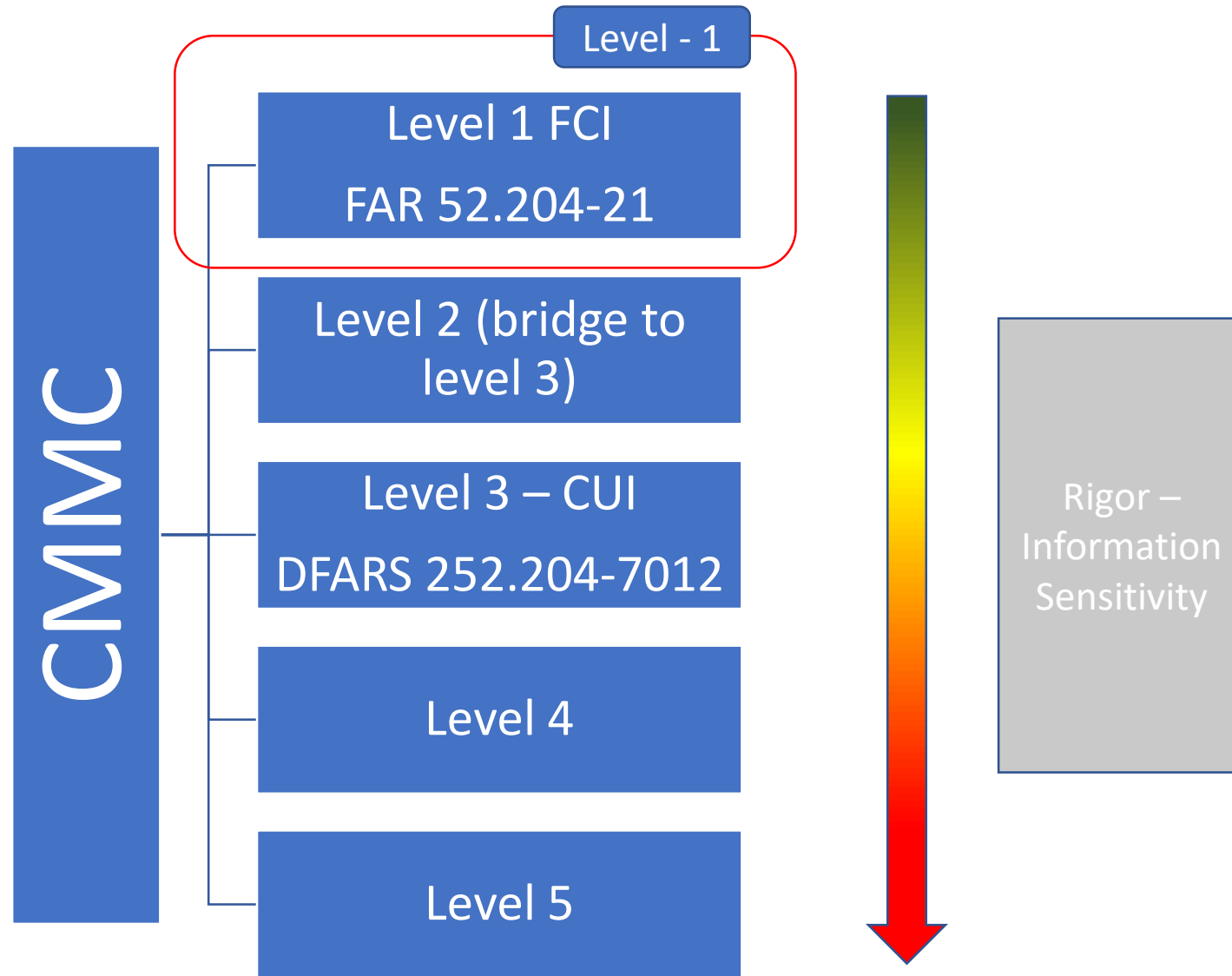


Figure 2. CMMC Levels and Descriptions

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

6/12/2020



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)

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

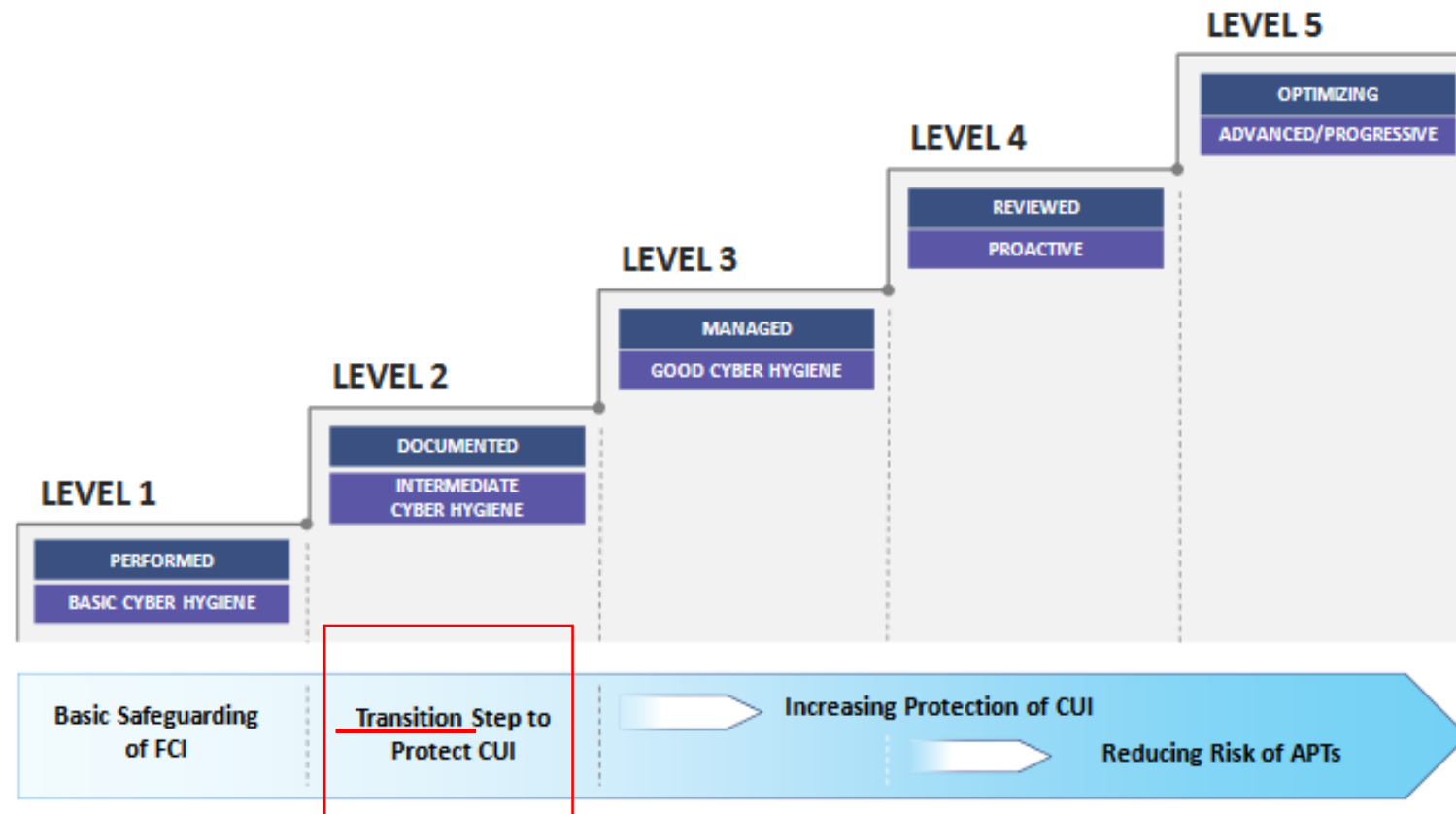


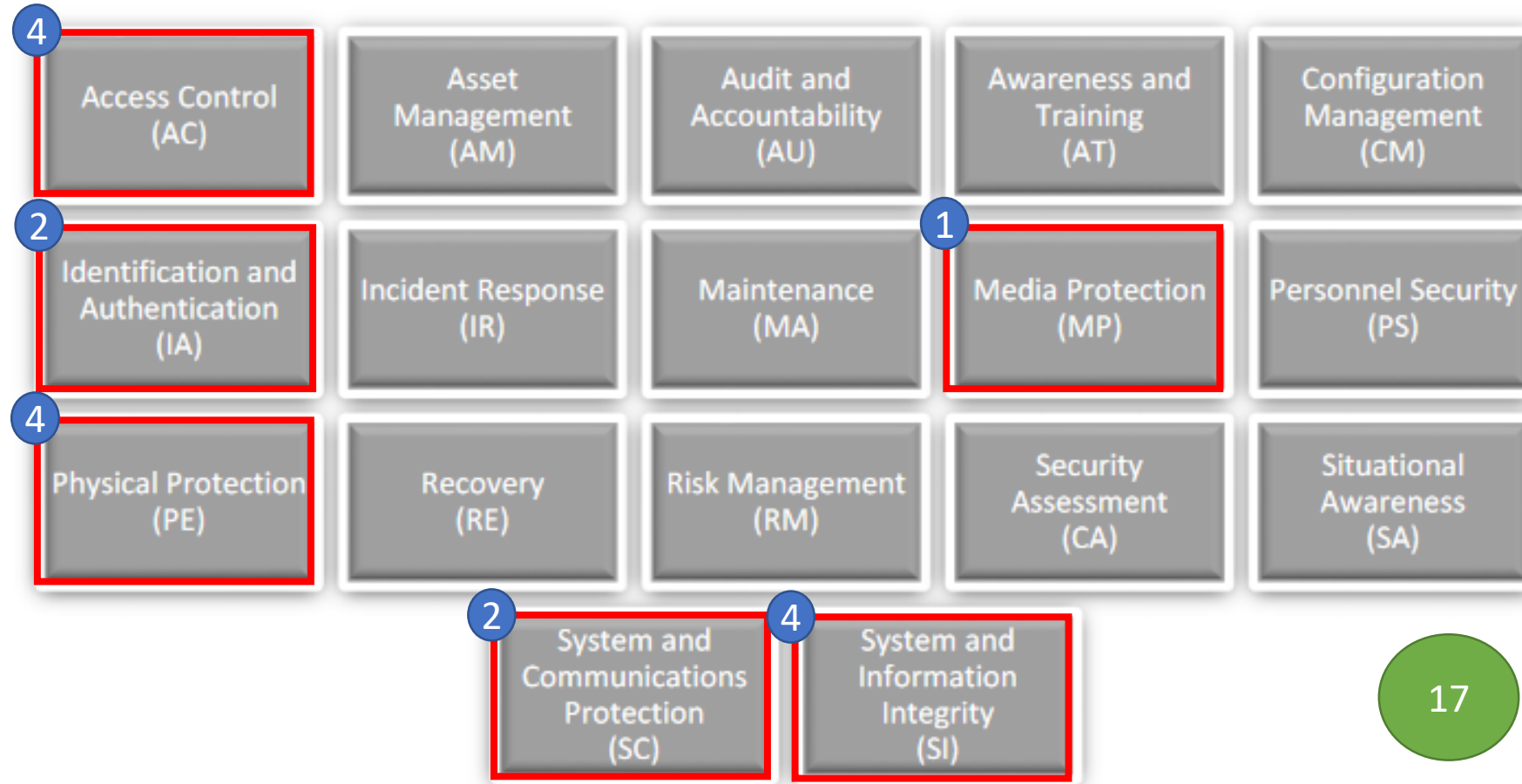
Figure 3. CMMC Levels and Associated Focus

6/12/2020

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.

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

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].

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.

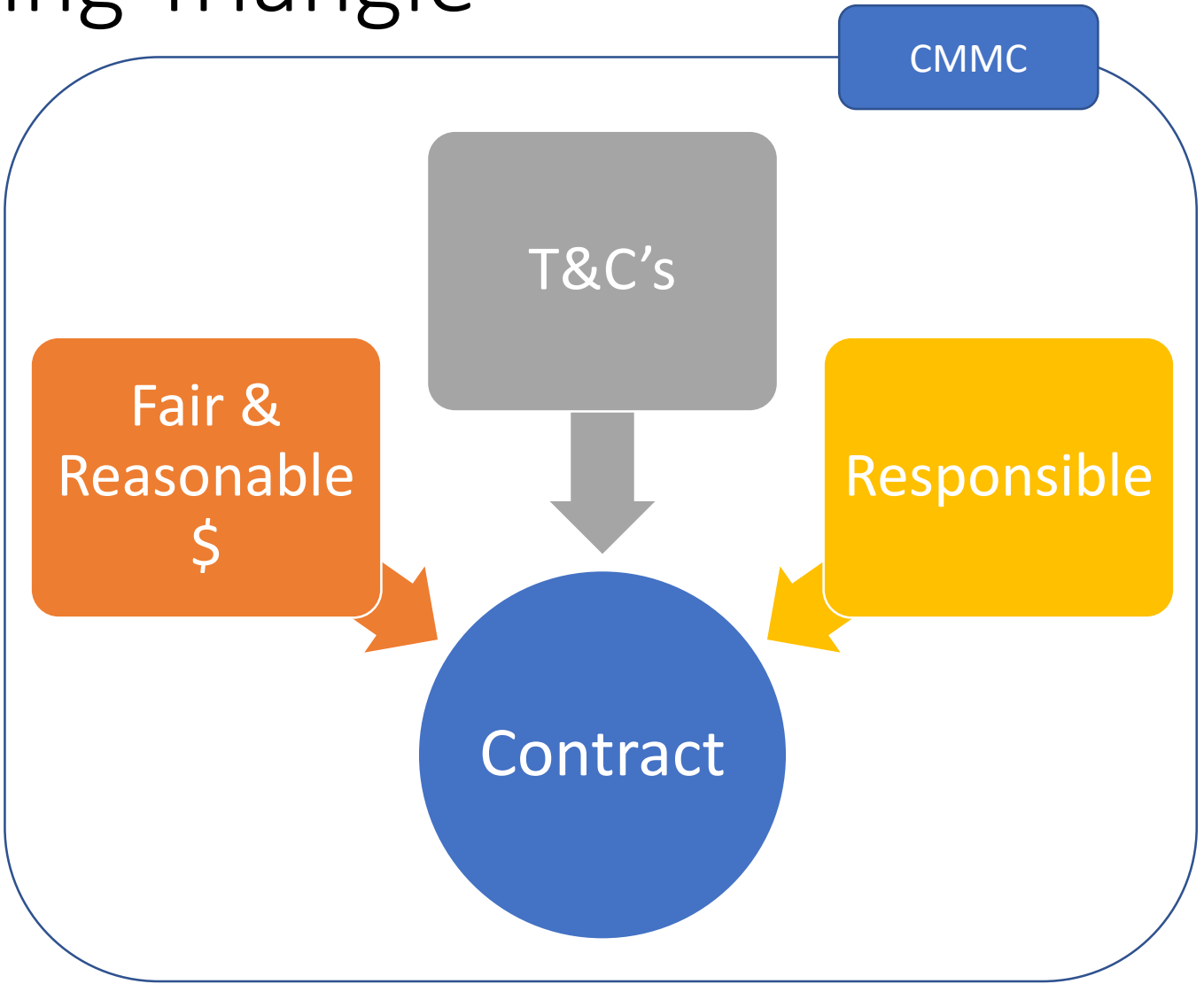
- Practices:

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].

Considerations for Certification

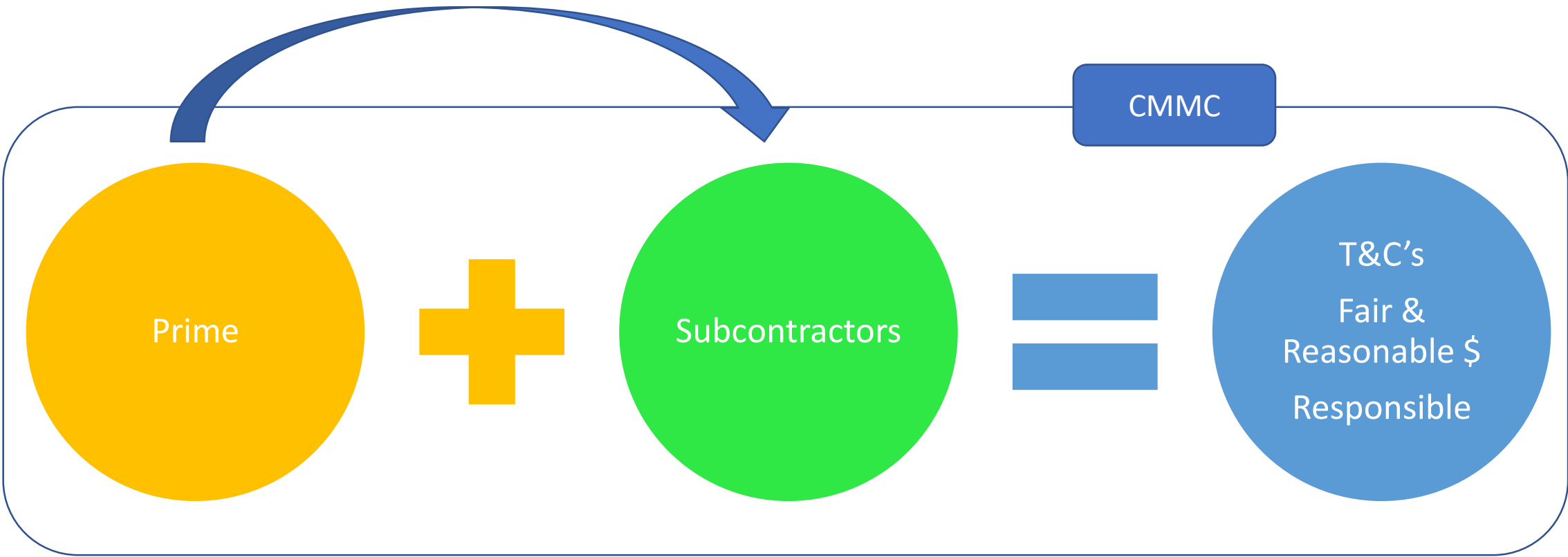
- An official visitor contacts the company for the purpose of reviewing your cyber policies and procedures (CMMC).
- A meeting is set up.
- What do you provide this individual?
- What documentation should you be keeping and be able to provide?
- Should there be training records?
- How do these policies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

Contracting Triangle



6/12/2020

Contracting Equation



Commonalities

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

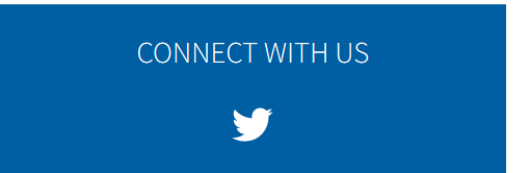


Cybersecurity Framework v1.1**

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

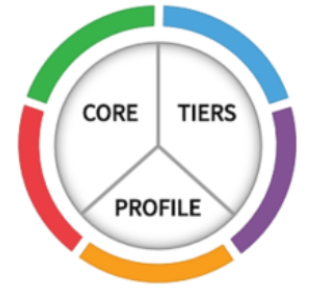
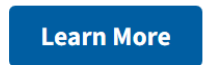
Cybersecurity Framework

- 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.

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.

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 versus 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.

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	<p>SECURITY REQUIREMENT</p> <p>Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).</p>
	<p>DISCUSSION</p> <p>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 versus non-privileged) are addressed in requirement 3.1.2.</p>

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 <i>Determine if:</i>
3.1.1[a]	<i>authorized users are identified.</i>
3.1.1[b]	<i>processes acting on behalf of authorized users are identified.</i>
3.1.1[c]	<i>devices (and other systems) authorized to connect to the system are identified.</i>
3.1.1[d]	<i>system access is limited to authorized users.</i>
3.1.1[e]	<i>system access is limited to processes acting on behalf of authorized users.</i>
3.1.1[f]	<i>system access is limited to authorized devices (including other systems).</i>
	POTENTIAL ASSESSMENT METHODS AND OBJECTS <u>Examine:</u> [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]. <u>Interview:</u> [SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities]. <u>Test:</u> [SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

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

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.

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

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**)

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

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>

UPCOMING TRAINING - 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*

ACQUISITION HOUR LIVE WEBINARS SERIES

« All Events

- *** NEW DATE * ACQUISITION HOUR: INTELLECTUAL PROPERTY FOR GOVERNMENT CONTRACTORS & SUBCONTRACTORS & THE STTR/SBIR STAKEHOLDER**

June 16 @ 1:00 pm - 2:00 pm

<https://www.wispro.org/event/intellectual-property-for-government-contractors-and-subcontractors-and-the-sttr-sbir-stakeholder/>

- 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 14, 2020

The SBA 8(a) Certification Program

[CLICK HERE](#) for additional information

Presented by Shane Mahaffy, US Small Business Administration (SBA)

- July 15, 2020

Responding to Sources Sought and Capabilities Statements

[CLICK HERE](#) for additional information

Presented by Mark Dennis, Wisconsin Procurement Institute (WPI)

ACQUISITION HOUR LIVE WEBINARS SERIES

- July 22, 2020

The HUBZone Certification Program

[CLICK HERE](#) for additional information

Presented by Shane Mahaffy, US Small Business Administration (SBA)

- August 25, 2020

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

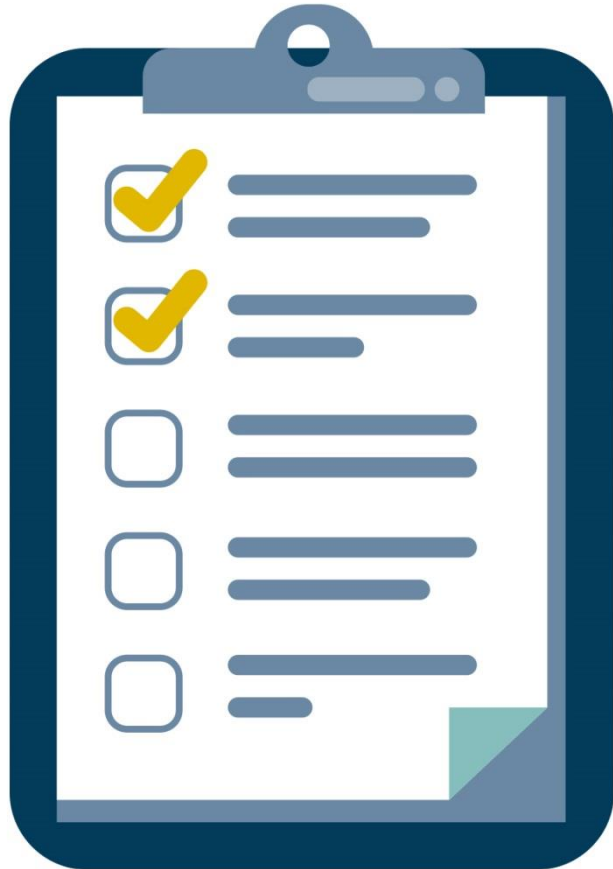
[CLICK HERE](#) for additional information

Presented by Shane Mahaffy, US Small Business Administration (SBA) and Mark Dennis,
Wisconsin Procurement Institute (WPI)

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