Wisconsin Procurement Institute

A Procurement Technical Assistance Center (PTAC)

THE PATH TO CMMC LEVEL 3

Acquisition Hour Webinar

August 26, 2020




ABOUT WPI
SUPPORTING THE MISSION

Celebrating 32 Years of serving Wisconsin Business!

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

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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

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

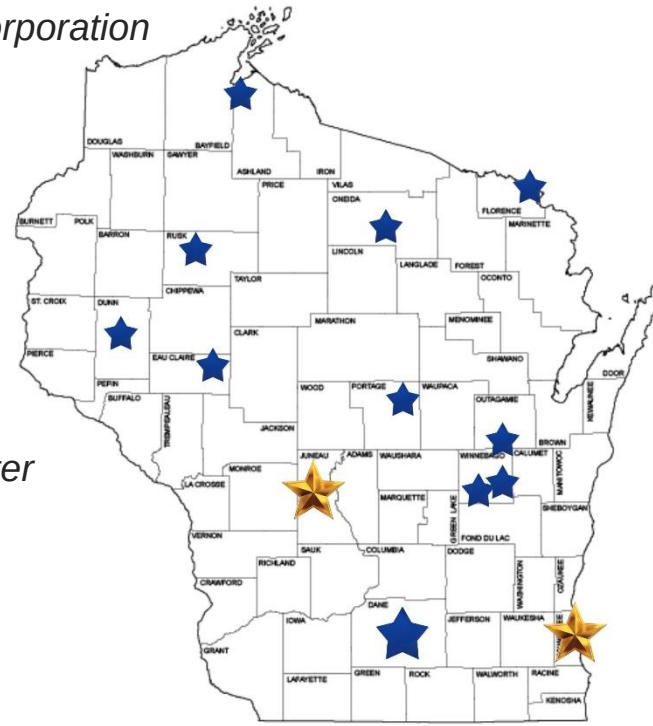
Last year WPI provided training at over 100 events and provided service to over 1,200 companies

WPI is a Procurement Technical Assistance Center (PTAC) funded in part by the Defense Logistics Agency (DLA), WEDC and other funding sources.

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

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*
- **FLORENCE**
  - *Florence County Economic Development*
- **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*
- **ASHLAND**
  - *Ashland Area Development Corporation*



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

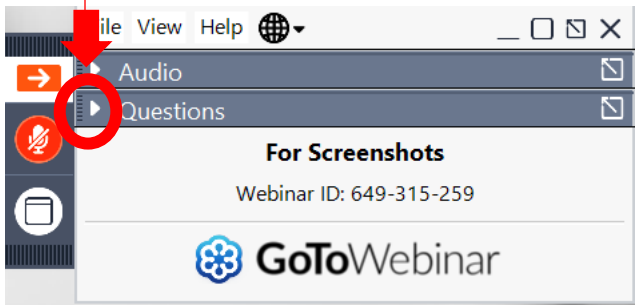
8/26/20


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.

QUESTIONS?

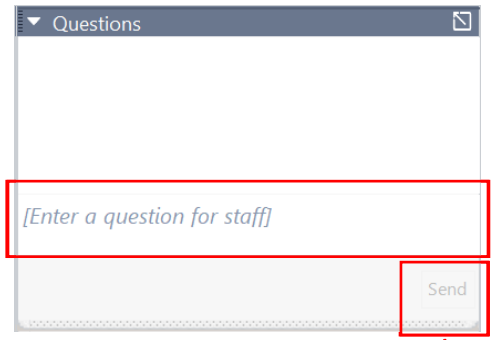
OPENING THE QUESTIONS BOX

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)

The Path to CMMC – Level 3

Marc N. Violante

August 26, 2020

Wisconsin Procurement Institute
A Procurement Technical Assistance Center (PTAC)

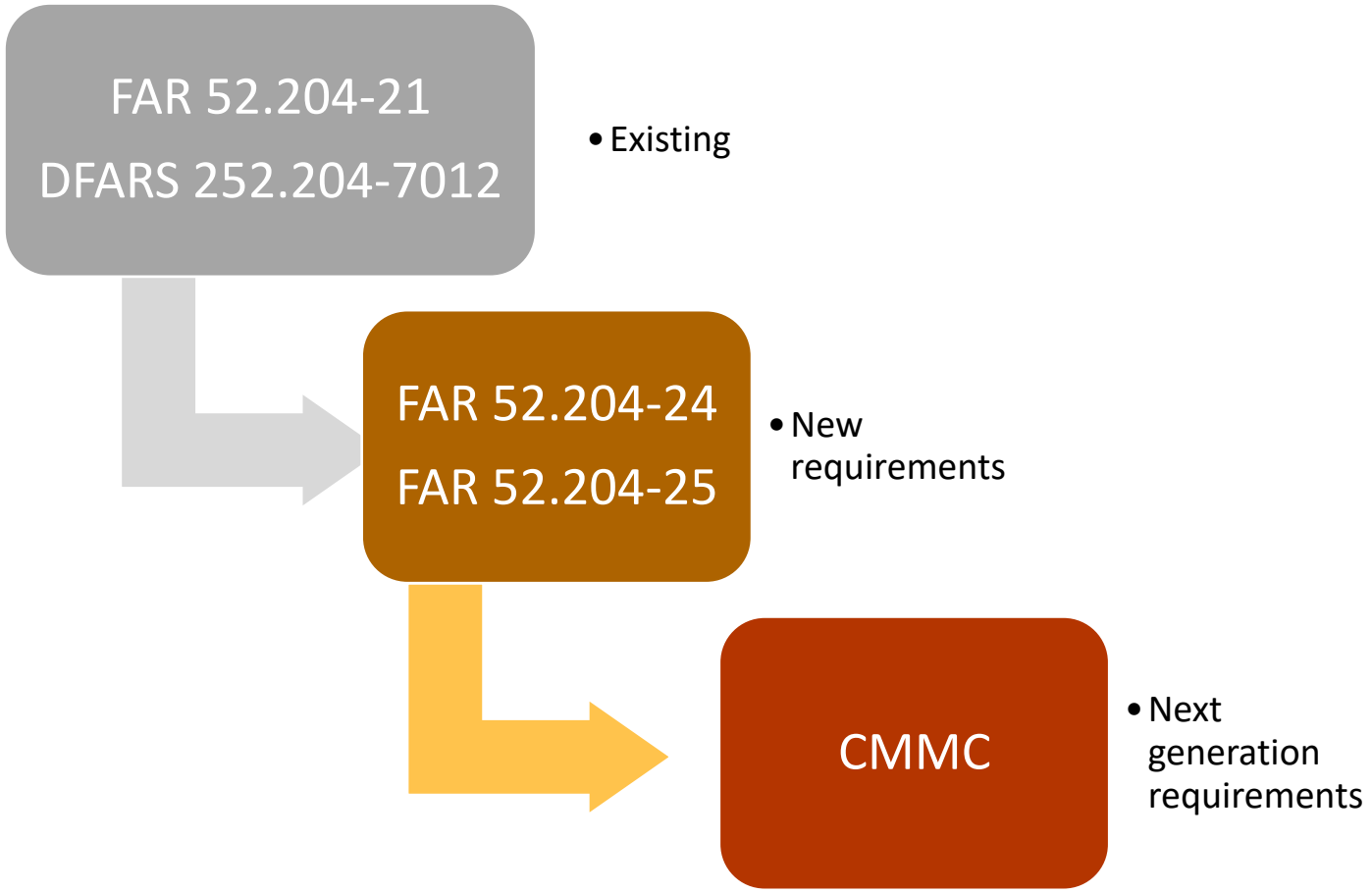
What we know - Current Cyber Obligations

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.

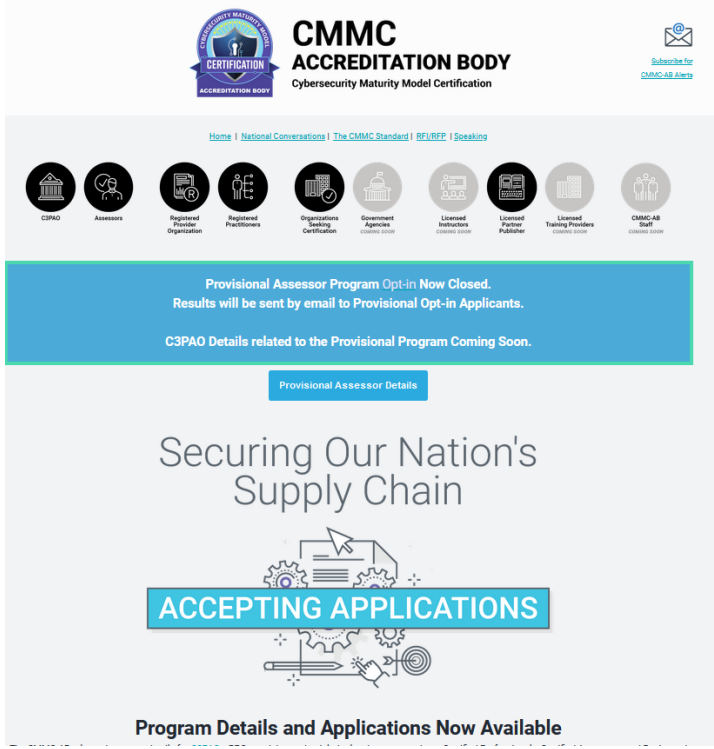
Requirements evolution – in part (related)



The Path to CMMC L3

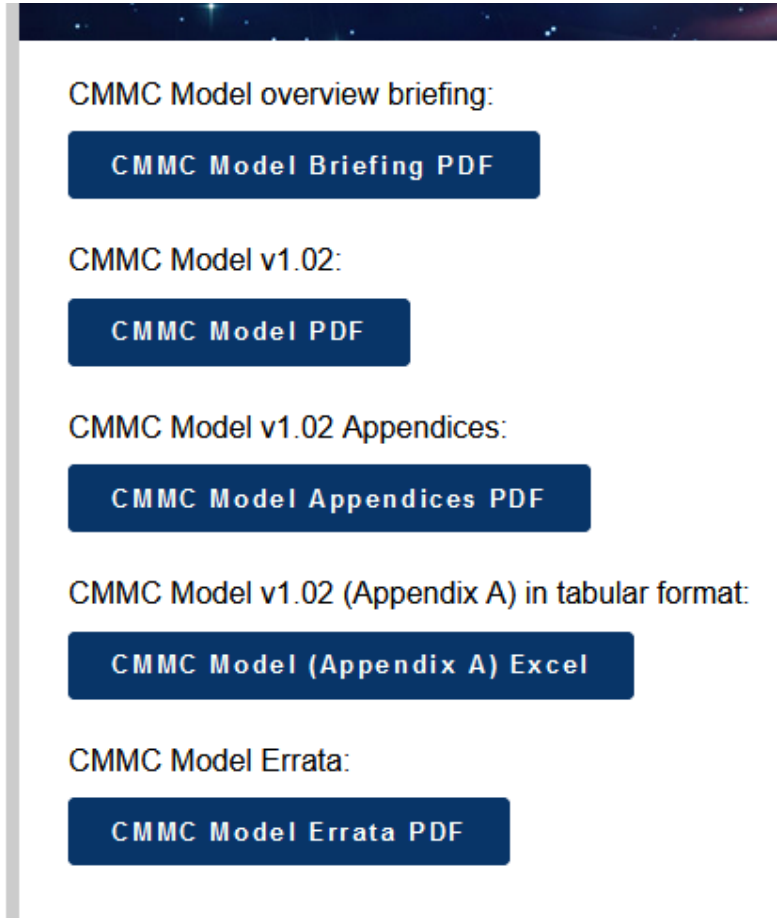
CMMC - Resources

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



https://www.cmmcab.org/

CMMC - Model



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

What we don’t know

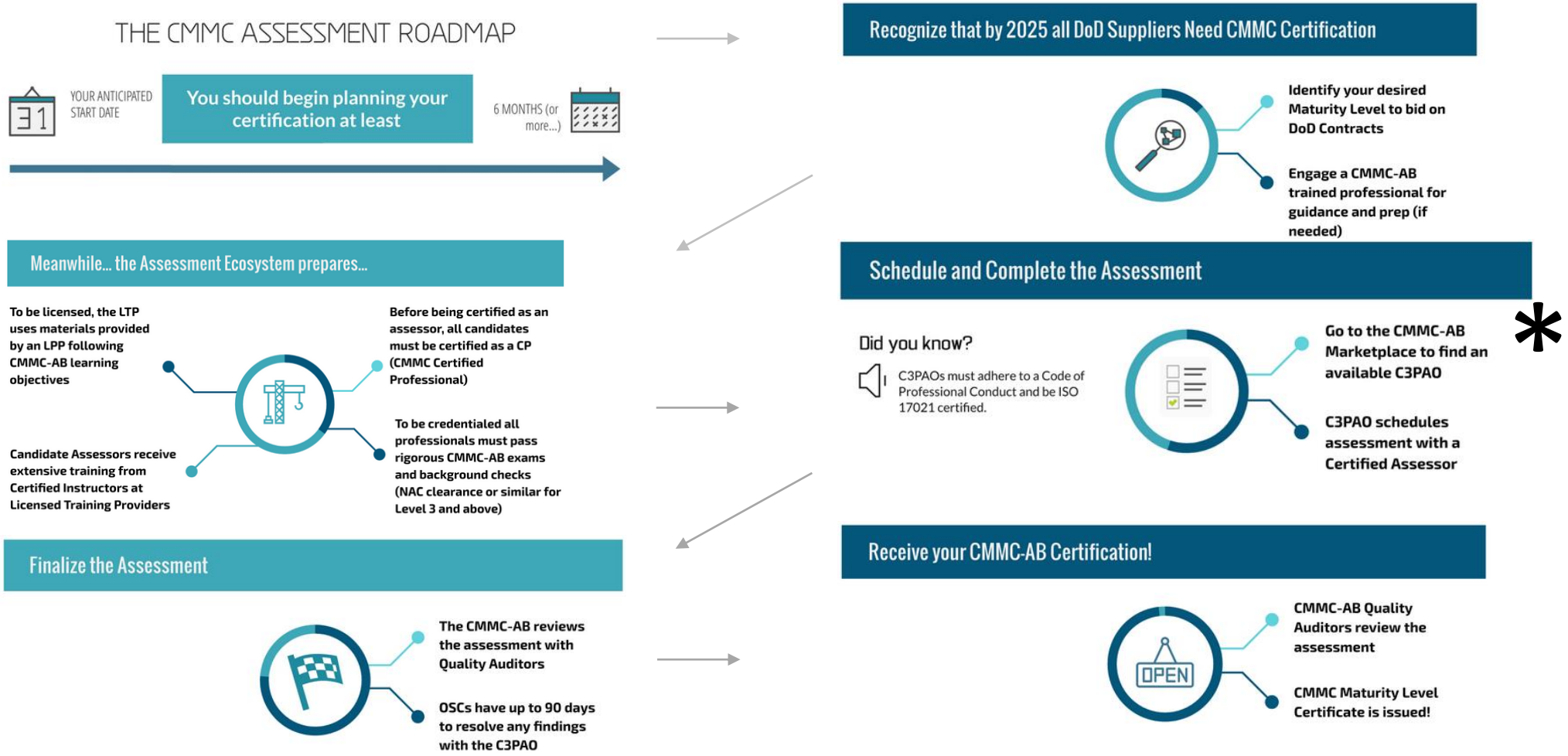
- How will the CMMC review be managed for L3?
- Will it be broken into sublevel reviews (L1 – L3)?
- If a company has previously undergone a certification for L1 or L2 – what then?

CMMC – Organizations Seeking Certification

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

THE CMMC ASSESSMENT ROADMAP

The path is just now being defined

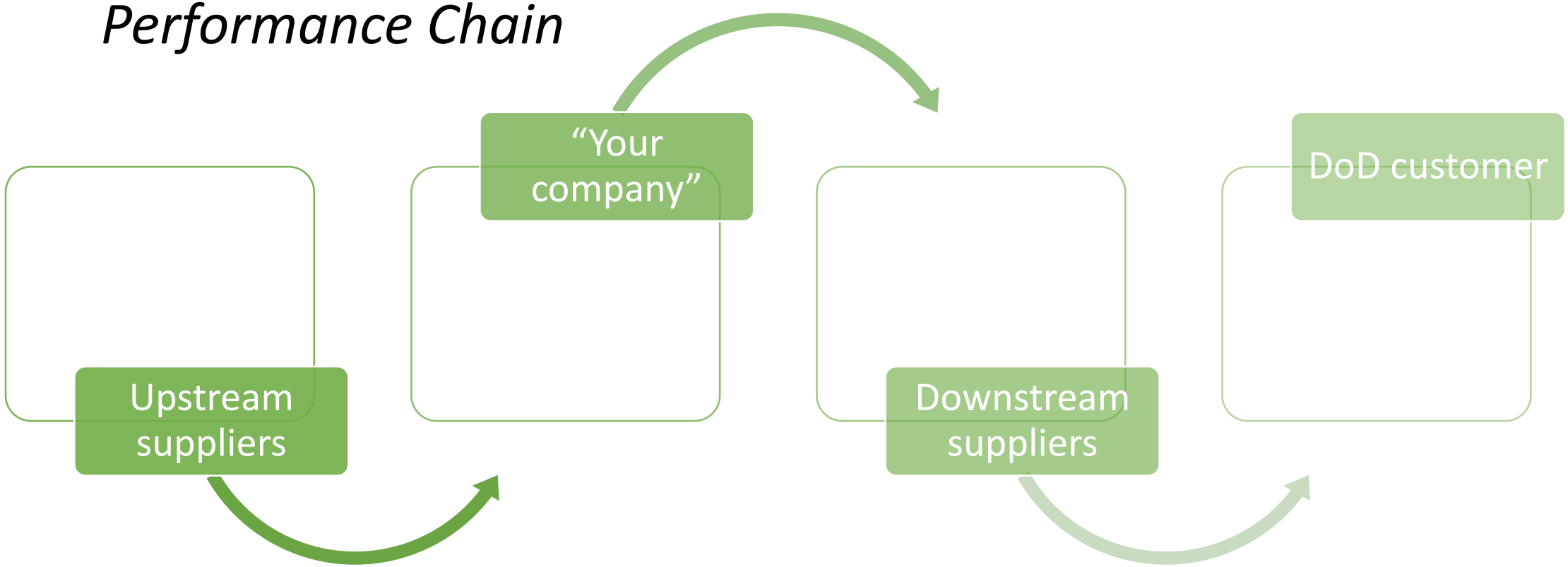


*

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

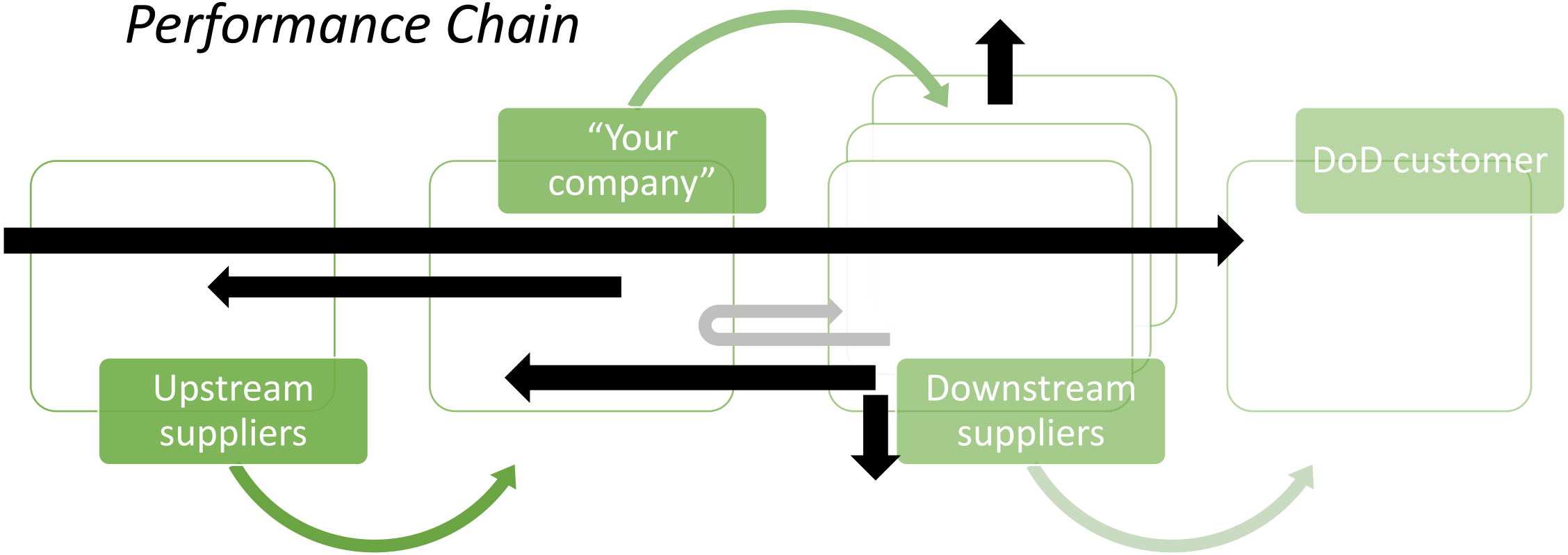
Key Idea – Supply Chain – Not company

Performance Chain

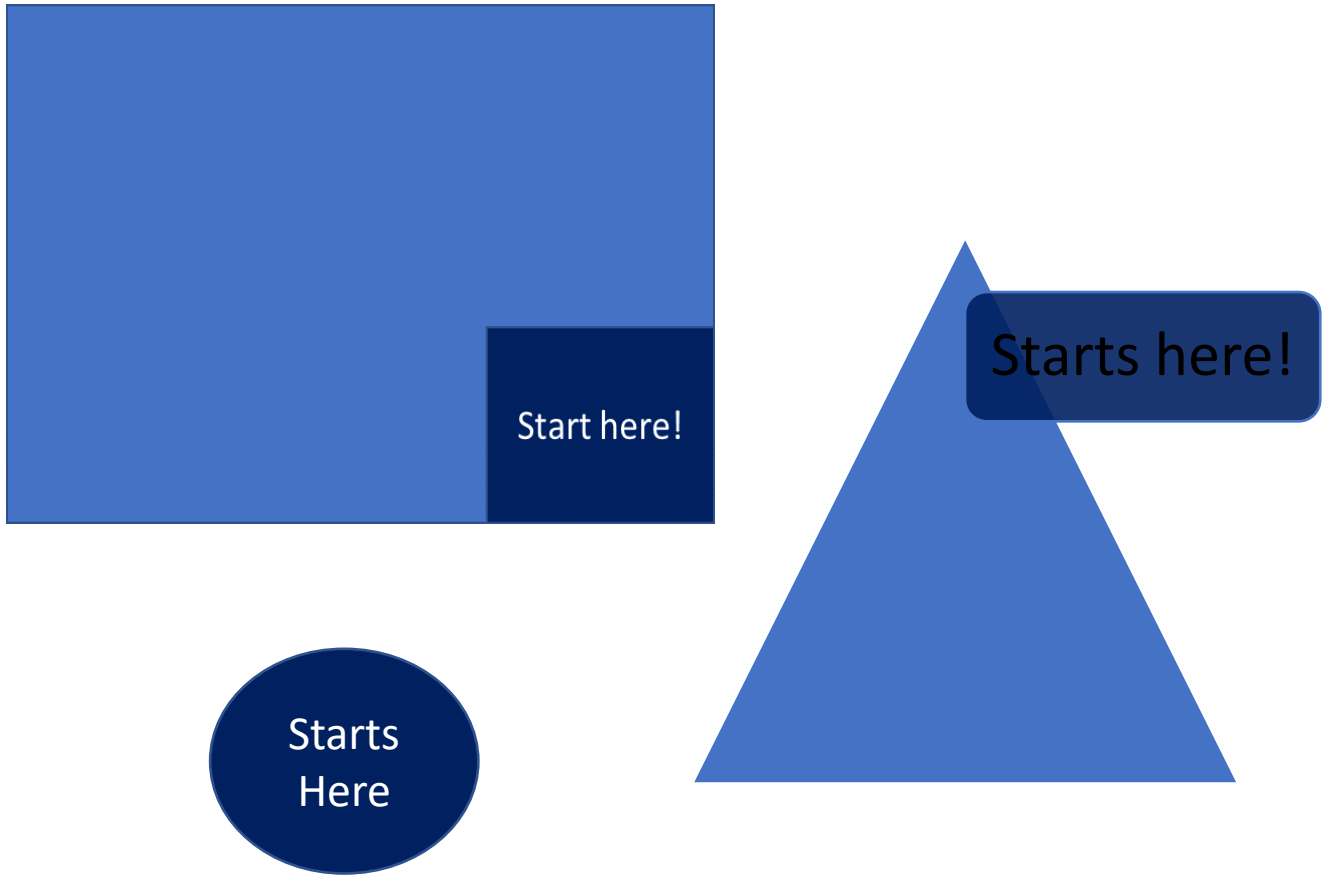


– Cyber Impacts

Performance Chain



The Path starts at the Top



- Support
- Resources
  - Funding
  - Staff
  - Talent
  - Upgrades
  - Training

What can CEOs do to mitigate cybersecurity threats?

- What is the threshold for notifying executive leadership about cybersecurity threats?
- What is the current level of cybersecurity risk for our company?
- What is the possible business impact to our company from our current level of cybersecurity risk?
- What is our plan to address identified risks?
- What cybersecurity training is available for our workforce?
- What measures do we employ to mitigate insider threats?
- How does our cybersecurity program apply industry standards and best practices?
- Are our cybersecurity program metrics measureable and meaningful?
- How comprehensive are our cybersecurity incident response plan and our business continuity and disaster recovery plan?
- How often do we exercise our plans?
- Do our plans incorporate the whole company or are they limited to information technology (IT)?
- How prepared is my business to work with federal, state, and local government cyber incident responders and investigators, as well as contract responders and the vendor community?

https://us-cert.cisa.gov/ncas/tips/ST18-007

Understand CMMC - goals

As part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DoD is working with industry to enhance the protection of the following types of unclassified information within the supply chain:

- *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].

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

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

Cause and Effect

- “Adversaries know that in today's great power competition environment, information and technology are both key cornerstones and -- and attacking a sub-tier supplier is far more appealing than a prime.
- “ We know that the adversary looks at our most vulnerable link, which is usually six, seven, eight levels down in the supply chain. So right now, there are a number of primes who have come up with some ideas about how to more cost-effectively accredit small and medium businesses.”
- “CMMC is a critical element of DOD's overall cybersecurity implementation. ”

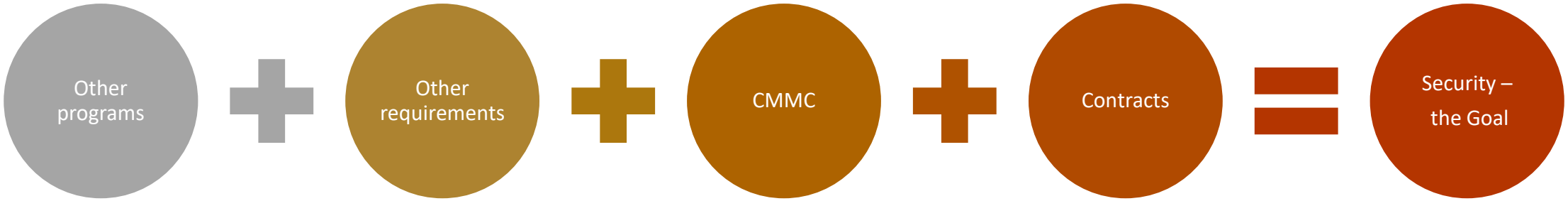
Ellen M. Lord, Assistant Secretary of Defense for Acquisition, Press Briefing transcript, January 31, 2020

Additional consideration

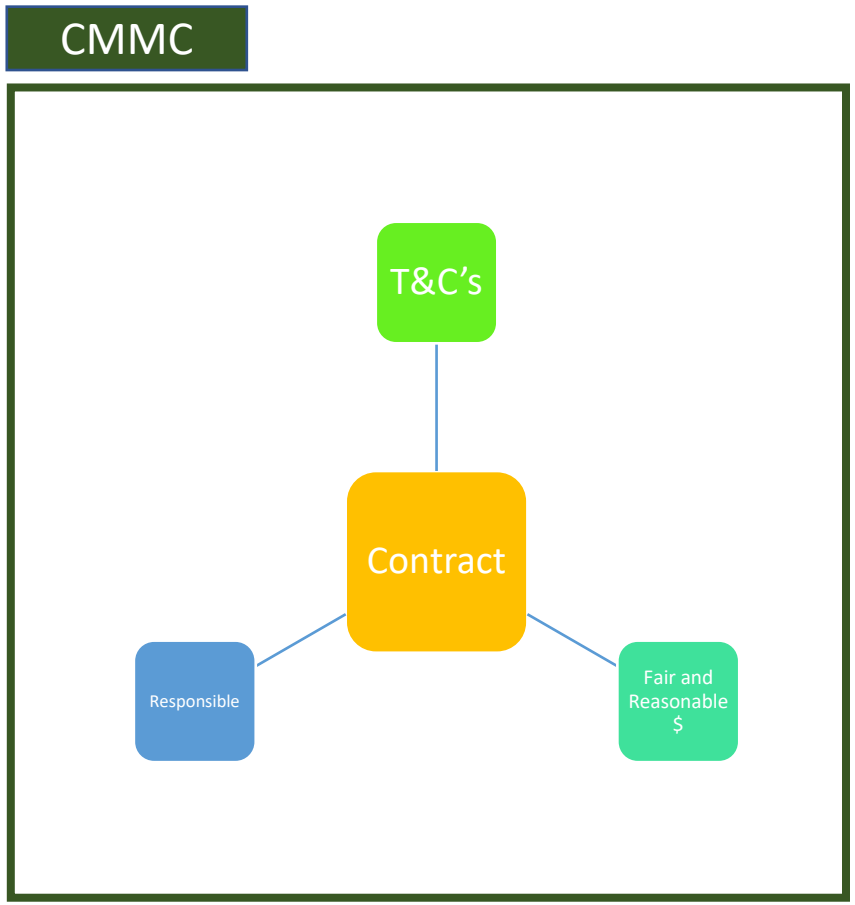
- Global interest - countries considering adoption of CMMC
  - Canada
  - United Kingdom
  - Denmark
  - Italy
  - Sweden
  - Poland
  - Israel
  - EU
  - Australia
  - Singapore

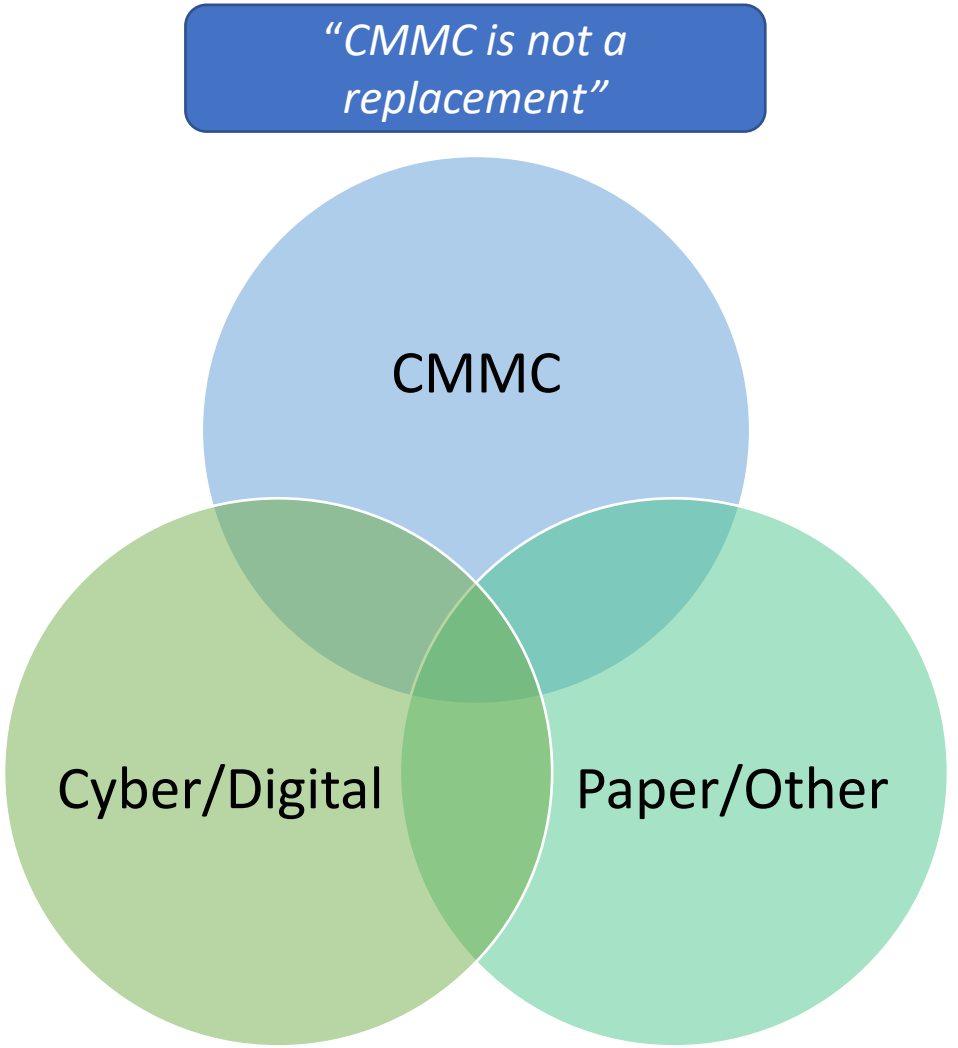
DOD Focuses on Minimizing Cyber Threats to Department, Contractors; Aug. 13, 2020 | BY C. Todd Lopez , DOD News – Ms. Lord's remarks to PSC

System Overview

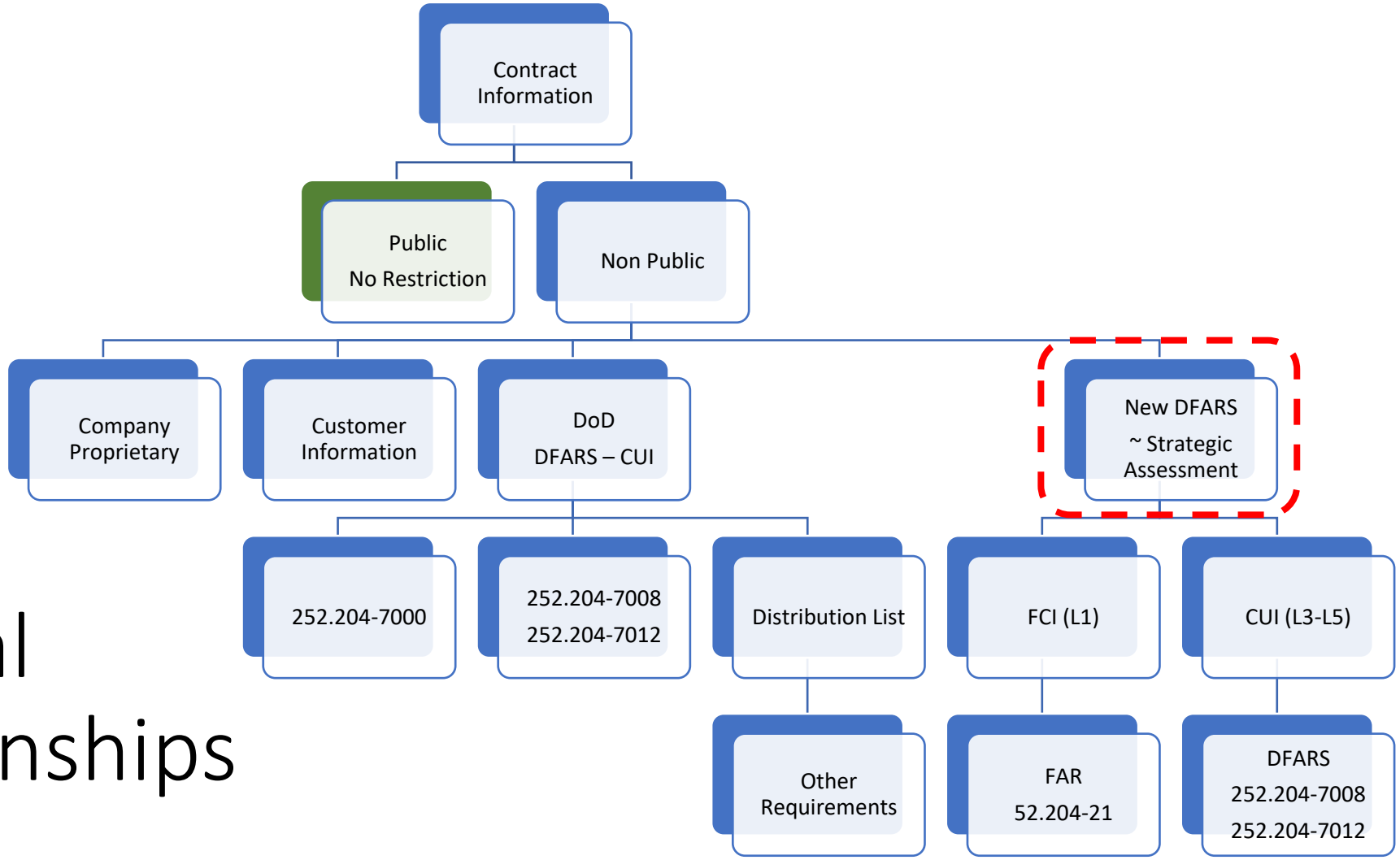


Program Relationships





General Relationships



New DFARS – Strategic Assessment & Cybersecurity Certification Requirements

Open DFARS Cases as of August 21, 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.

https://aaf.dau.edu/

Adaptive Acquisition Framework & the 5000 series

"The Adaptive Acquisition Framework will be the most transformational acquisition policy change we've seen in decades."

Ms. Ellen Lord, USD(A&S)

Integrates the New 5000 Policies

The 5000 series policies were updated to reflect the new set of key tenets of the Defense Acquisition System with new policies for each acquisition pathway and functional area. This AAF website integrates the policies, guides, and resources for the acquisition workforce to navigate their program lifecycle.

See all the Policies and Guides

https://aaf.dau.edu/

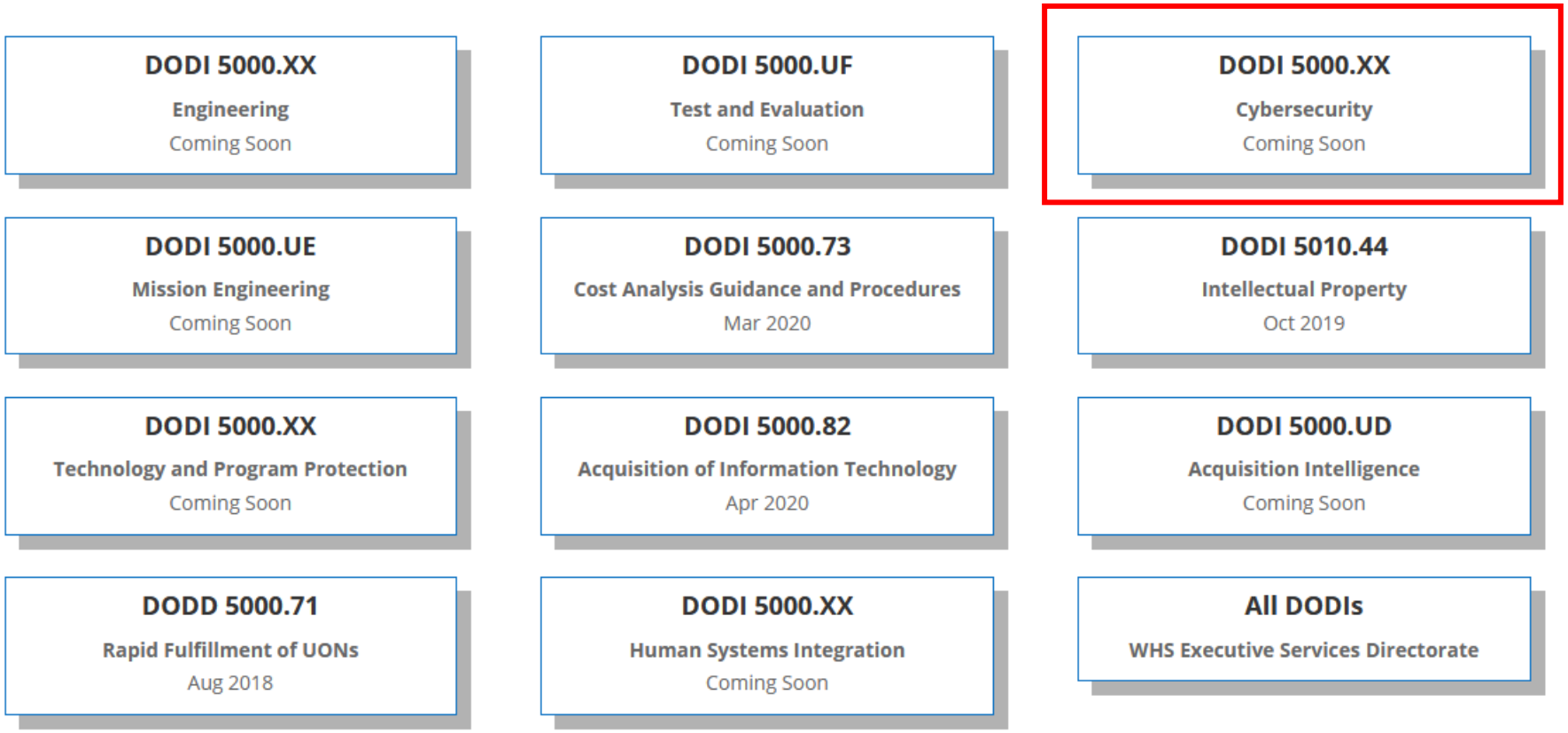
Resources, perspective, information

Table 1. Relationship of DoDI 5000.02T and New Policy, continued

Enclosure 10. Cost Estimating and Reporting	Necessary guidance is available in DoDI 5000.73, "Cost Analysis Guidance and Procedures." Removal of this enclosure is in progress.
Enclosure 11. Requirements Applicable to All Programs Containing Information Technology (IT)	DoDI 5000.82, "Acquisition of Information Technology (IT)"
Enclosure 12. Urgent Capability Acquisition	DoDI 5000.UB, "Urgent Capability Acquisition"
Enclosure 13. Cybersecurity in the Defense Acquisition System	• Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) DoDI 5000.CS, "Cybersecurity for Acquisition Decision Authorities and Program Managers" • Under Secretary of Defense for Research and Engineering (USD(R&E)) technology and program protection issuance in development

https://aaf.dau.edu/

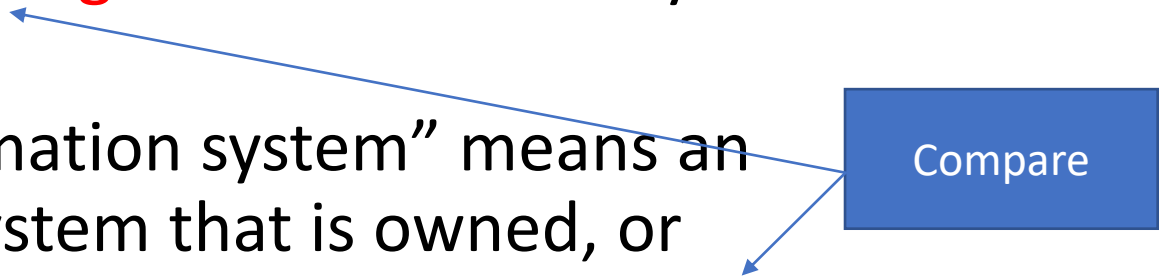
Adaptive Acquisition Framework & the 5000 series



https://aaf.dau.edu/

Apply definitions – track source dates

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



Information Security Obligations/Requirements

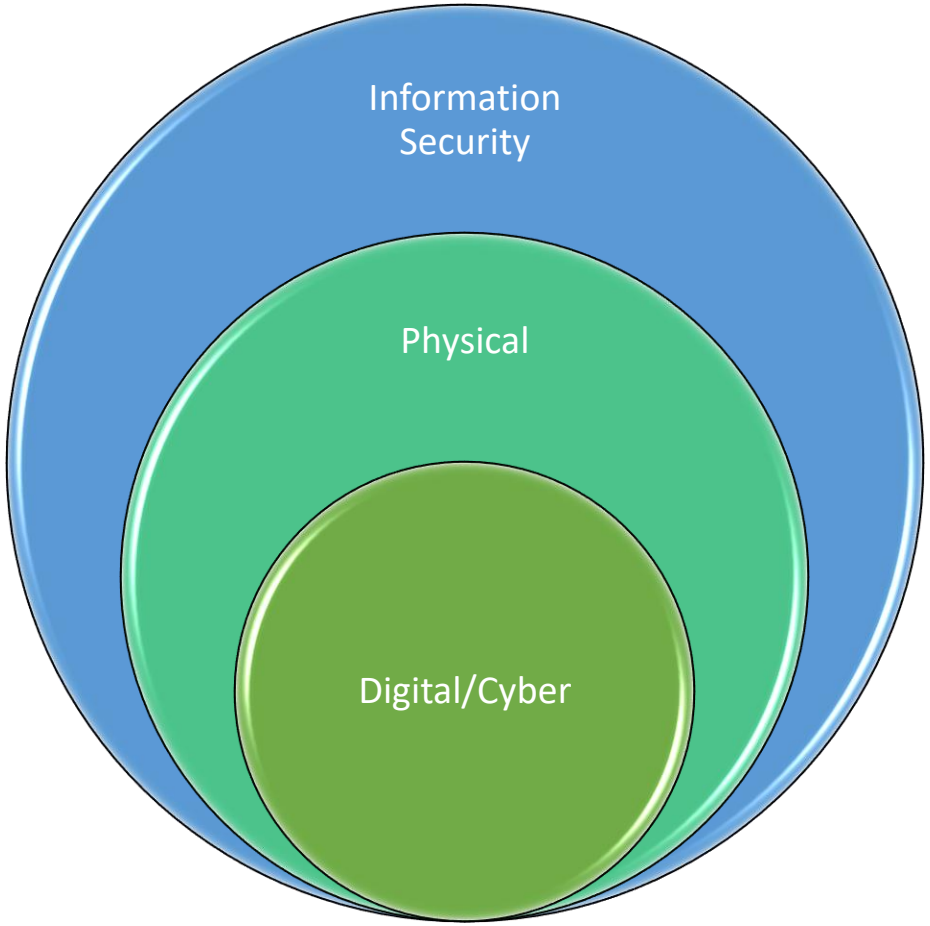
Equally Important & Related

- 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

Various categories are routinely 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



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)

Information categories

- Federal Contract Information
- Controlled Unclassified Information
- Critical Defense Information
- ITAR
- JCP
- NOFORN
- Distribution List
- Navy Nuclear
- Customer Proprietary
- Company Proprietary

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

CMMC – includes various media & paper

MEDIA PROECTION (MP)

CAPABILITY	PRACTICES			
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	
C022 Identify and mark media			MP.3.122 Mark media with necessary CUI markings and distribution limitations. • NIST SP 800-171 Rev 1 3.8.4 • NIST CSF v1.1 PR.PT-2 • CERT RMM v1.2 MON:SG2.SP4 • NIST SP 800-53 Rev 4 MP-3	
C023 Protect and control media		MP.2.119 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. • NIST SP 800-171 Rev 1 3.8.1 • NIST CSF v1.1 PR.PT-2 • CERT RMM v1.2 KIM:SG2.SP2 • NIST SP 800-53 Rev 4 MP-4	MP.3.123 Prohibit the use of portable storage devices when such devices have no identifiable owner. • NIST SP 800-171 Rev 1 3.8.8 • NIST CSF v1.1 PR.PT-2 • CERT RMM v1.2 MON:SG2.SP4 • NIST SP 800-53 Rev 4 MP-7(1)	

CMMC v1.02; March 18, 2020

CMMC - clarification

CMMC CLARIFICATION

In this case, "media" can mean something as simple as paper, or storage devices like diskettes, disks, tapes, microfiche, thumb drives, CDs and DVDs, and even mobile phones. It is important to see what information is on these types of media. If there is Federal contract information (FCI)—information you or your company got doing work for the Federal government that is not shared publicly)—you or someone in your company should do one of two things before throwing the media away:

- clean or purge the information, if you want to reuse the device; or
- shred or destroy the device so it cannot be read.

See NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization for more information.

CMMC v1.02; March 18, 2020

Entity - abstraction

Facility/Office

Physical access points	People	Information	IT System (network)

• Doors
• Windows
• Bays
• Loading Docks
	• Staff
	• Visitors
	• Suppliers
	• Subcontractors
	• Official visitors
		• Physical
		• Digital
		
		• All formats
		• Communication channels - all
			• Wired/Wireless
			• Users
			  • Staff
			  • Visitors
			• Devices

Key Questions

- What information is handled?
- What are the handling/security requirements?
- Who is accessing?
- Is access limited?
- Is access based upon a “need to know?”

Initial Actions

- Identify all access points
- Identify access point controls and normal operations
- Compile list of authorized users
- Compile list of all devices – company – office & shop – all locations
- Compile list of personal devices authorized
- Review requirements – CMMC (1-3)
- Review – System Security Plan
- Review logs, log status, and use

Questions

- Are all documents marked?
- Has there been training that covers the proper handling of each classification of material?
- Has a Security Manager been formally designated?
- Has the Security Manager attended training?
- Is there a security management manual?
- How are updates handled?

Create/manage information census

- Identify –
  - Information held
  - Responsible individual
  - Location
  - Program
  - Storage requirements
  - Marking requirements
  - Sharing restrictions
  - Destruction requirements
  - Update records as needed

Conduct internal Census - Software

- Software
  - Licenses – fees, dates, other
  - Product specific/Open/Other
  - Copies – authorized, actual
  - Locations
  - Update – versions
  - Person – Responsibilities

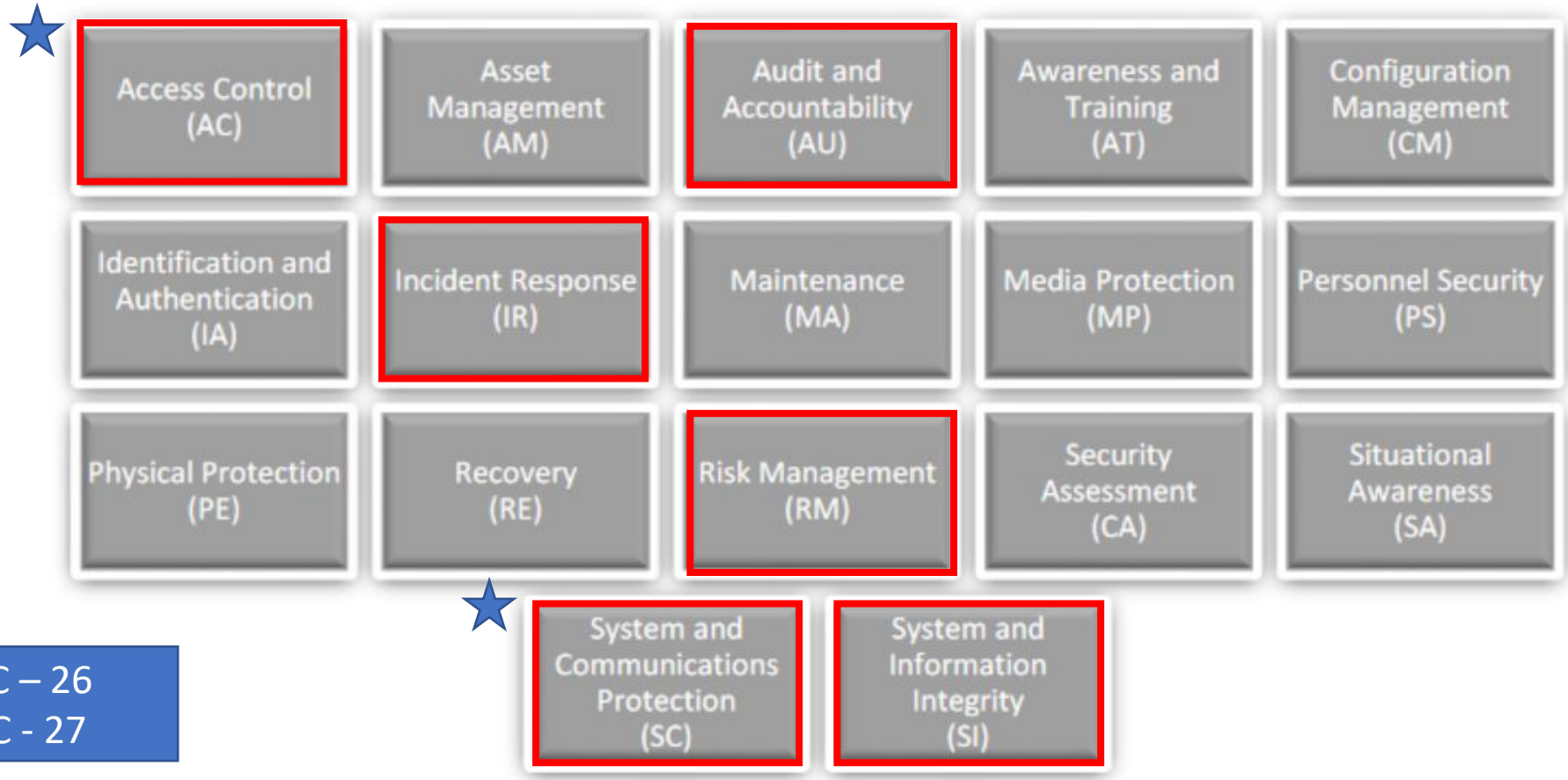
Subcontractors / Suppliers

- Does the company have a master list of information categories used and a matrix of handling/eligibility requirements?
- How are subcontractors/suppliers identified and selected?
  - Capability alone?
  - Eligibility for access to various information?
- What background information is collected on subcontractors/suppliers?
- What documentation exists?
- How is information “coded”, transmitted and managed?

Conduct internal Census – Access Lists/Logs

- Access lists
  - Who has access?
  - Permission/Authorization
- Logs
  - Frequency
  - Detail
  - Review requirements

The “Big Six” (105 of 171 practices)



AC – 26
SC - 27

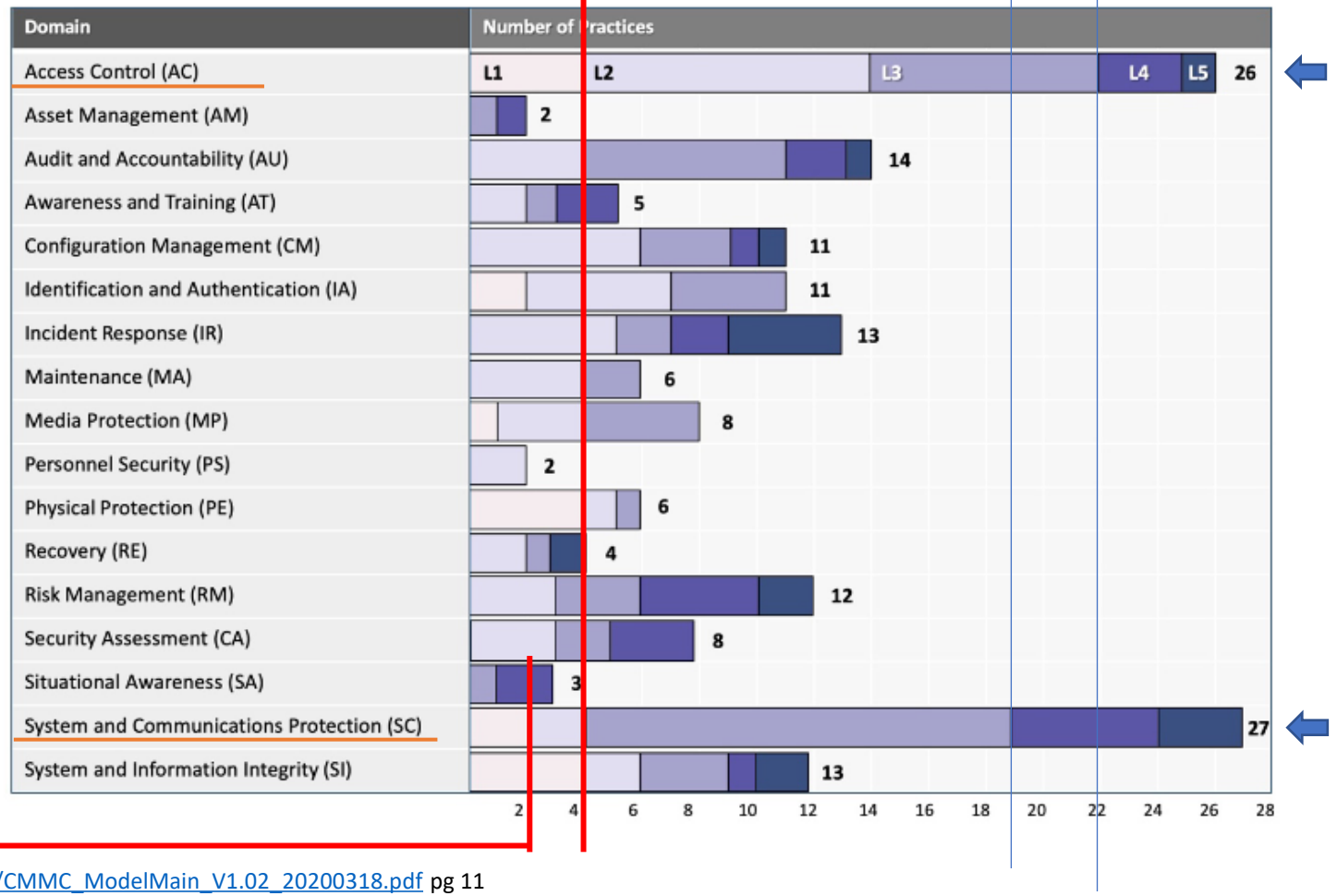
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf pg 11

Practices v. Domain v. Level

SC: L3 - 19

AC: L1 - 4

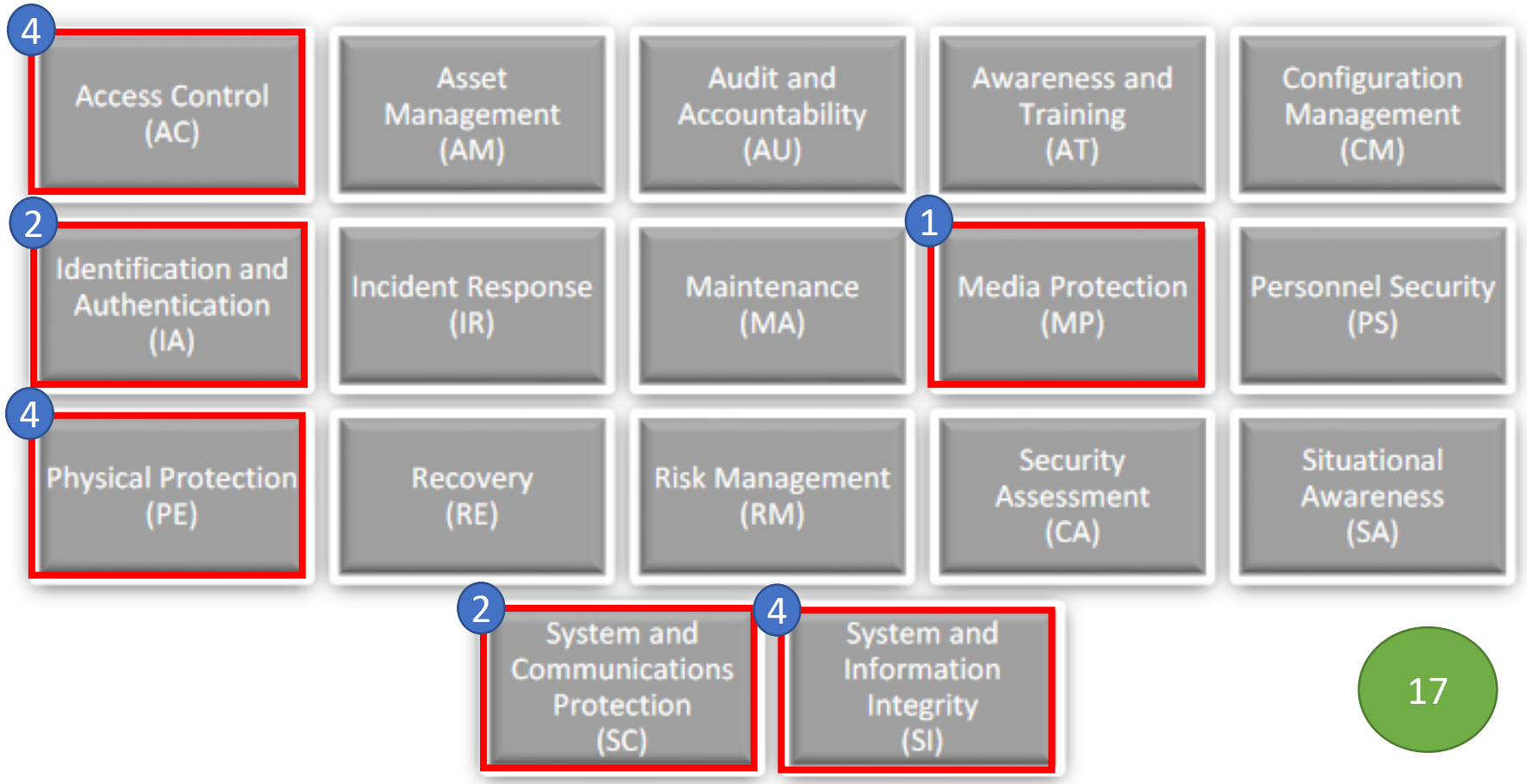
AC: L3 - 22



SC: L1 - 4

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

CMMC – Domains (Level-1)



Step 1

- CMMC – L1
  - Federal Contract Information
  - FAR 52.204-21
  - 15 requirements in FAR == 17 requirements in CMMC L1
  - List requirements
  - Assemble resources
  - Evaluate business processes and security
  - Identify GAPS

C001- Establish system access requirements –a

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

Become familiar with references

Specifications for Minimum Security Requirements

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

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

C001- Establish system access requirements – a1

- FAR Clause 52.204-21 b.1.i

(b) Safeguarding requirements and procedures.

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

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

- NIST SP 800-171 Rev 1 3.1.1

3.1 ACCESS CONTROL

Basic Security Requirements

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

3.1.1	**SECURITY REQUIREMENT** 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

Internal Actions

- Review requirements
  - Conduct R/Y/G Analysis
  - ID each element by CMMC Level and color
  - Group by level and color
- Develop notional timeline
- Assign Responsibilities
- Assemble Resources

What is a R/Y/G analysis

- Green –
  - Company capable – company managed
  - Example
- Yellow –
  - Internal/external
  - Example
- Red –
  - Outsourcing required
  - Example

Developing Policies

- 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.

https://www.acq.osd.mil/cmmc/docs/CMMC_Appendices_V1.02_20200318.pdf pg: B-2
CERT RMM v1.2 GG2.GP1 Subpractice 2

Some things

- Mindset
- Commitment
- Resources
- Awareness of programs and their requirements
- References
- Training
- Maintenance & updates

Documentation

- Complete
- Thorough
- Process to ID gaps – “holes”
- Seek – what has been overlooked
- Stay away from – “It’s always been that way” or
- That won’t happen to us
- Tested
- Tailored
- Process to update

Background

Why agencies need to prevent a classified spillage

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

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

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

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

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

Develop your key questions – such as:

- How do you know?
- How do you identify?
- How do you account for?
- How do you track?
- Who can access?
- Do you have processes and procedures?
- What records do you maintain/retain?
- How frequently do you test?

Establish and Maintain a Compliance Program

Program elements:

- Fully supported by senior management
- Regularly reviewed/updated
- Research & apply references
- Clearly documented in writing
- Tailored to the business
- Tailored to information being handled
- Training (periodic/as needed) conducted; documented
- Outward looking component – feedback, current external issues

Key management/security requirements

- Solicitation Review
- Identification of data/information requirements
- Identify team members
- Advise of requirements
- Create limited access space
- Control access, information and time (functional, specified, unlimited)
- Detail requirements – sharing, copying, transmission

Training

Train: Teach individuals the concepts to perform the functions within the organization and how to be an asset. Implement entry-level professional education. Ensure training is relevant and updated to keep pace with the changing environment.

cyber poses to successful mission accomplishment. The annual cybersecurity training, currently required by DoD, is insufficient in providing that training to the overall workforce. It is slow to change and does not sufficiently relate the threat to the individual in ways that are understandable and relevant to their jobs and the missions they are performing. Evaluating training effectiveness by simply clicking through electronic training that is virtually identical to the previous year does not increase user level knowledge or reduce risk.

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

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 WEBINAR SERIES

- 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. SBA 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)

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

8/26/20

- 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

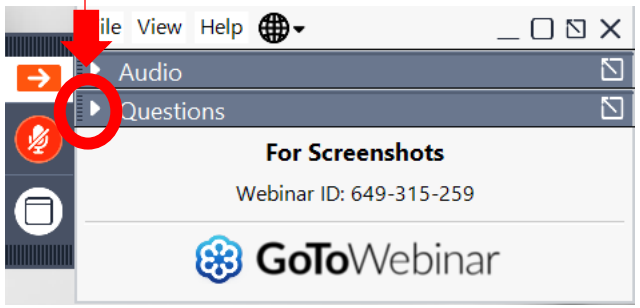
A CRITICAL NOTICE FROM WPI

- 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?

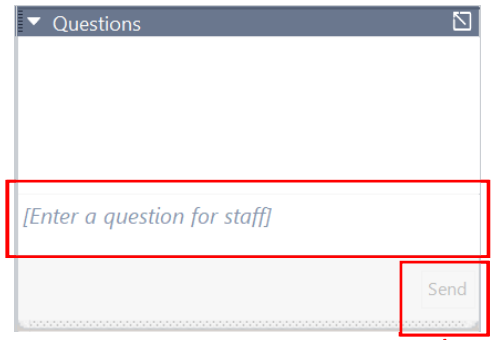
OPENING THE QUESTIONS BOX

Click here to access
within the Control Panel



USING THE QUESTIONS BOX

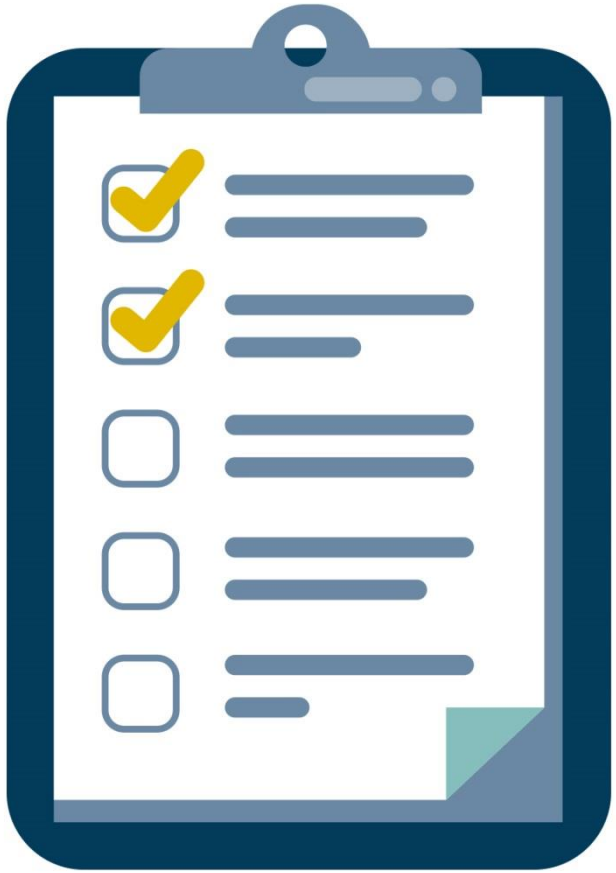
Type questions
here at any time
during a
presentation



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