SANS

Understanding CMMC Compliance for DoD Contractors

What is CMMC?

- Cybersecurity Maturity Model Certification (CMMC)
- Current version is CMMC v1.02, released March 2020
- Maintained by the Office of the Under Secretary of Defense for Acquisition & Sustainment

- Primary Documentation Includes:
  - CMMC Model Main (v1.02)
  - CMMC Assessment Guide – Level 1 (v1.10)
  - CMMC Assessment Guide – Level 3 (v1.10)
  - NIST SP 800-171 / 800-171A

Why was CMMC Created?

- Originally all DoD contractors were responsible to comply with NIST SP 800-171 (Jan 2018)
- However, compliance was often measured through self-certification and self-assessment
- When audits were performed, many contractors who self-certified did not pass their audits

- CMMC was created to be a DoD acquisitions tool to ensure that organizations handling CUI met a baseline for cybersecurity

Who is Responsible to Comply with CMMC?

- Organizations storing, processing, or transmitting sensitive DoD data as a part of a DoD acquisition project must comply
- Each acquisition will specifically describe the level of certification required
- This includes both the Prime and any subcontractors

Data Type Handled	Certification Level Required
Public Information Only	No Certification Required
Federal Contract Information (FCI)	CMMC Level 1 Certification
Controlled Unclassified Information (CUI)	CMMC Level 3, 4, or 5 Certification

Controlled Unclassified Information (CUI)

- The CUI program is a US federal program meant to consolidate the practices used to manage *sensitive unclassified information*

- Originally a recommendation of the 9/11 report (2004), was codified in Executive Order 13556 (2010)
- National Archives and Records Administration (NARA) is responsible for guidance and enforcement of the order

- A full list of categories of data covered by the CUI program can be found at: https://www.archives.gov/cui/registry/category-list

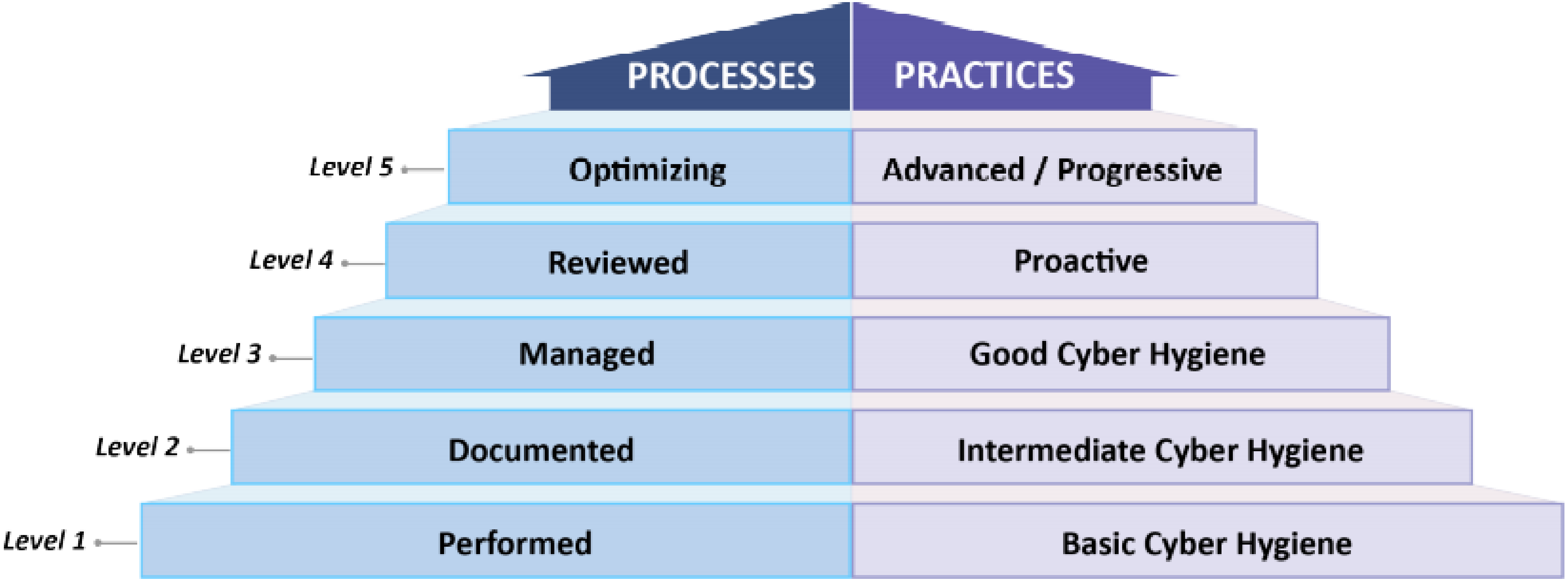
CUI Covered Organizational Groups (Categories)

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax

Organizations Not Handling CUI

- Some organizations responsible for Federal Contract Information (FCI) will not handle CUI
- Handling CUI includes storing, processing, or transmitting CUI
- Organizations not handling CUI, but responsible for FCI, will be responsible for certifying at a minimum of CMMC level 1
- Organizations that are purely COTS software developers do not

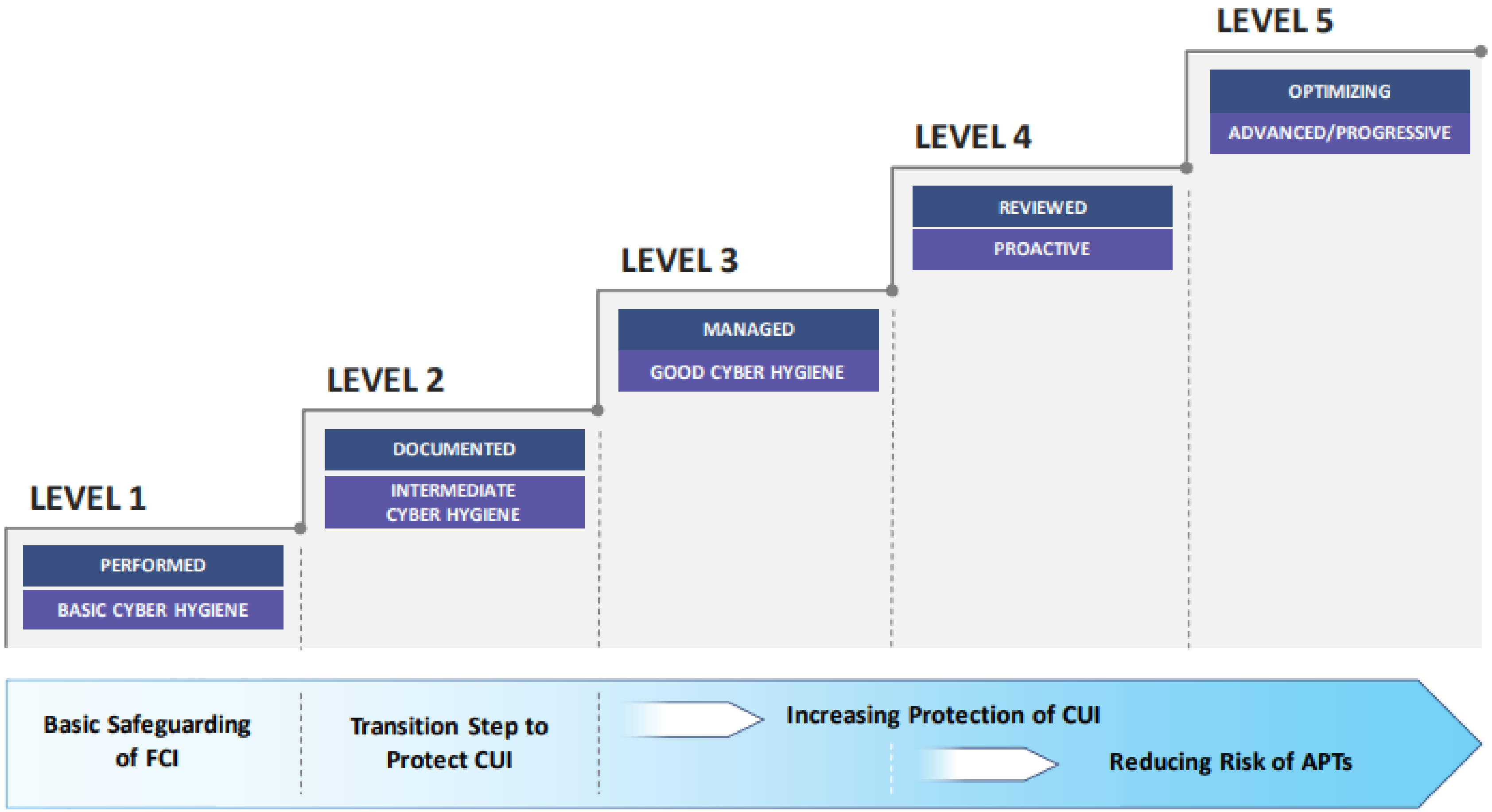
CMMC Levels and Descriptions



	PROCESSES	PRACTICES
Level 5	Optimizing	Advanced / Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

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

CMMC Levels and Focus



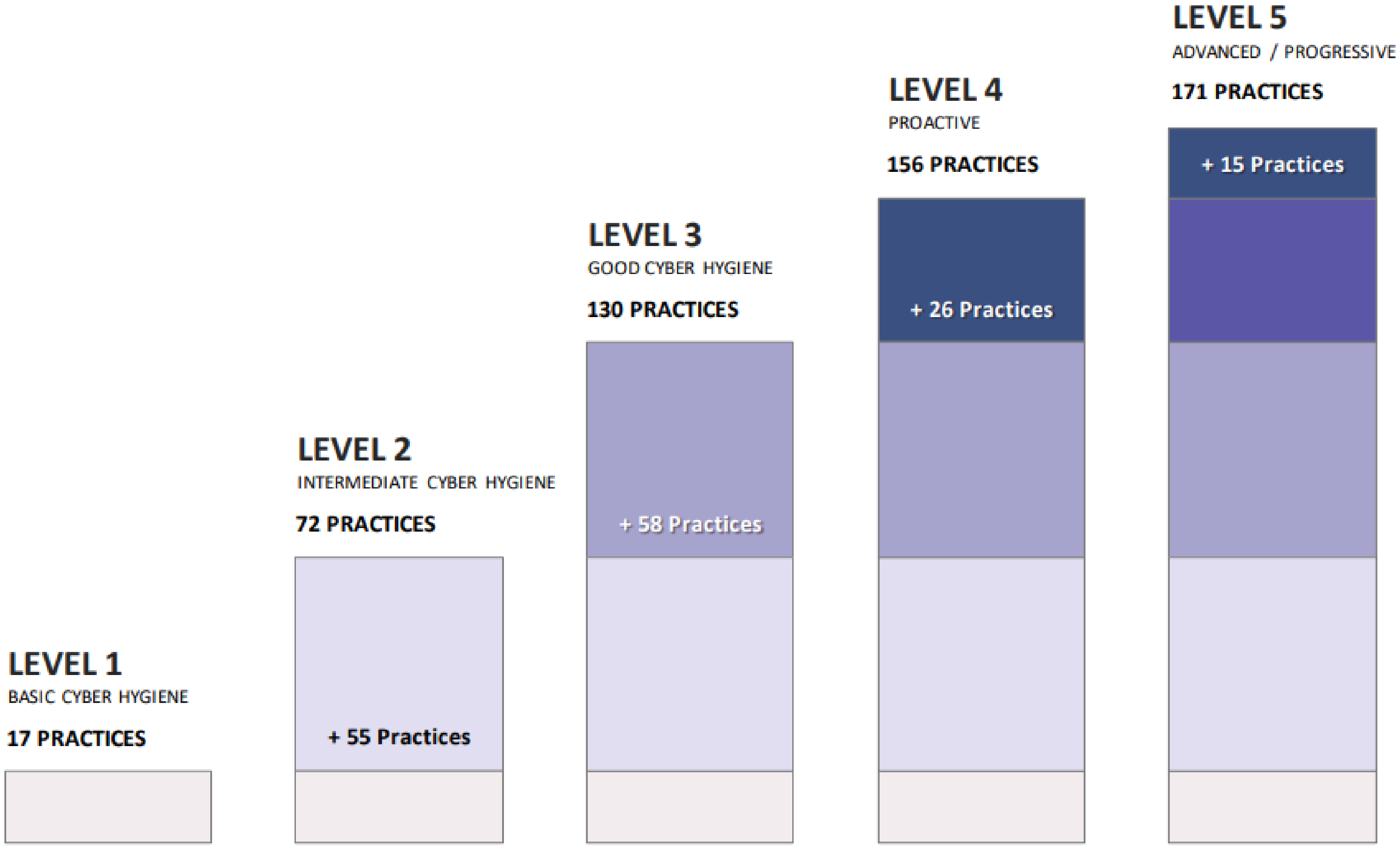
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

CMMC Domains

- Access Control (AC)
- Asset Management (AM)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

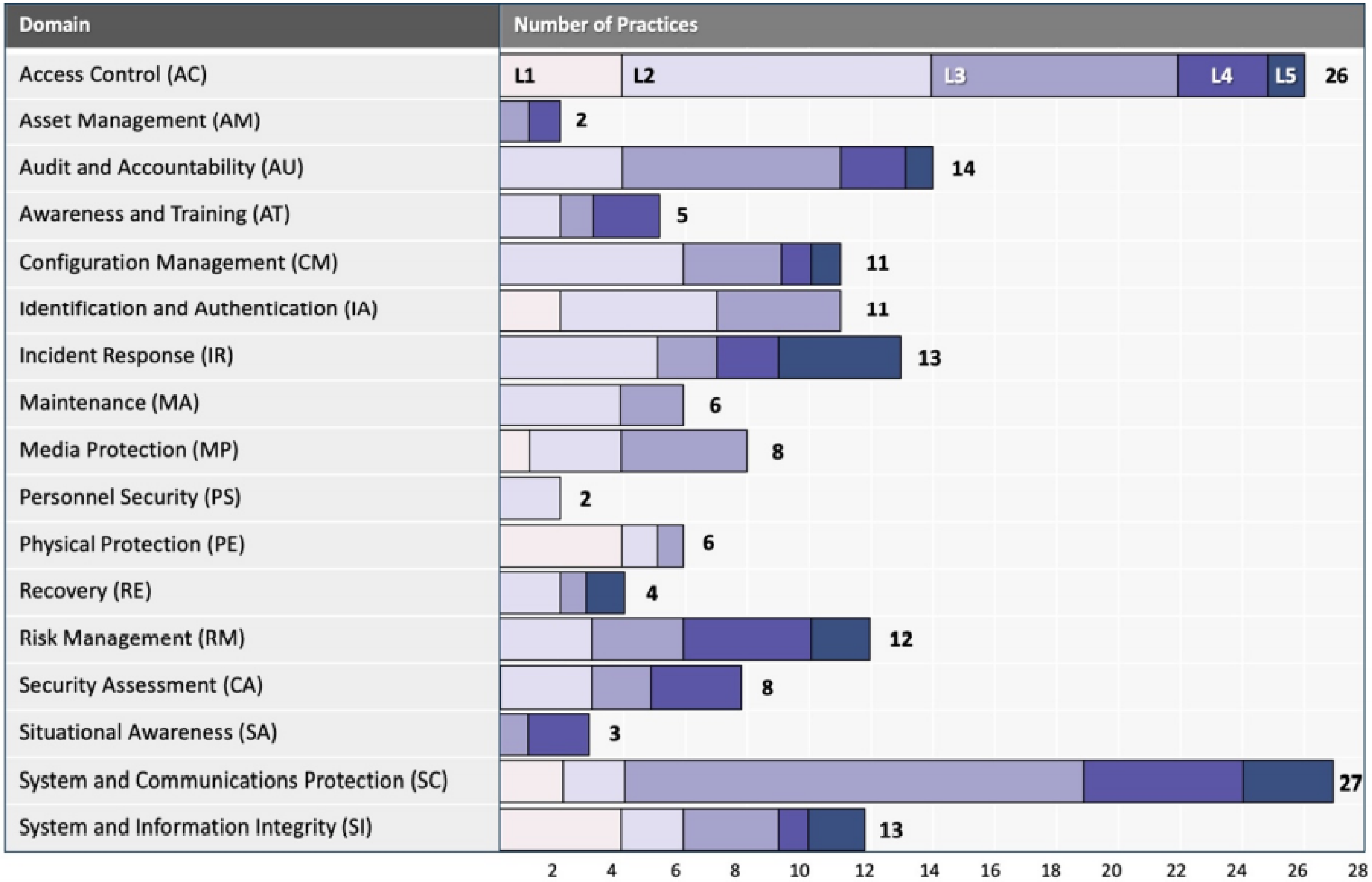
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

CMMC Practice by Level



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

CMMC Practices by Domain



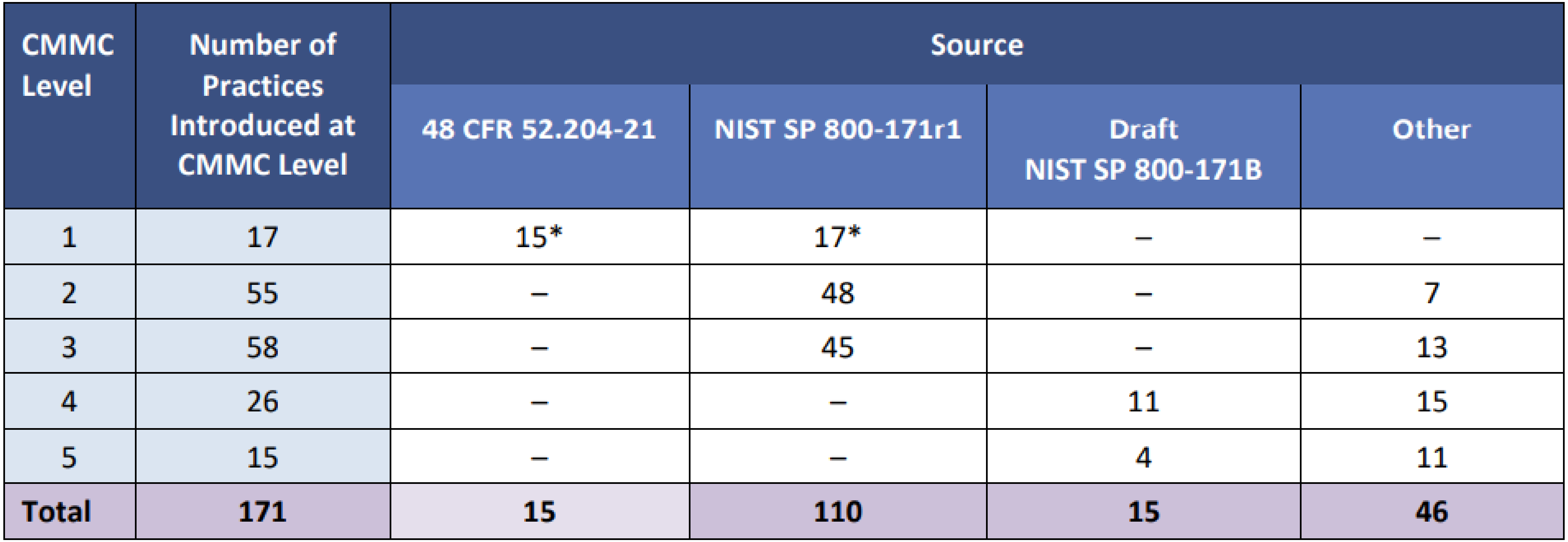
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

DFARS 252.204-7012 vs NIST SP 800-171 (rev2) vs CMMC Practices

- There are clear similarities between the control libraries
- CMMC level 3 contains the 110 controls found in NIST 800-171

- Additional controls have also been added to CMMC from:
  - NIST SP 800-53
  - Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933
  - Center for Internet Security (CIS) Controls
  - Computer Emergency Response Team (CERT) Resilience Management Model (RMM)

DFARS vs NIST SP800-171 vs CMMC Practices



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**

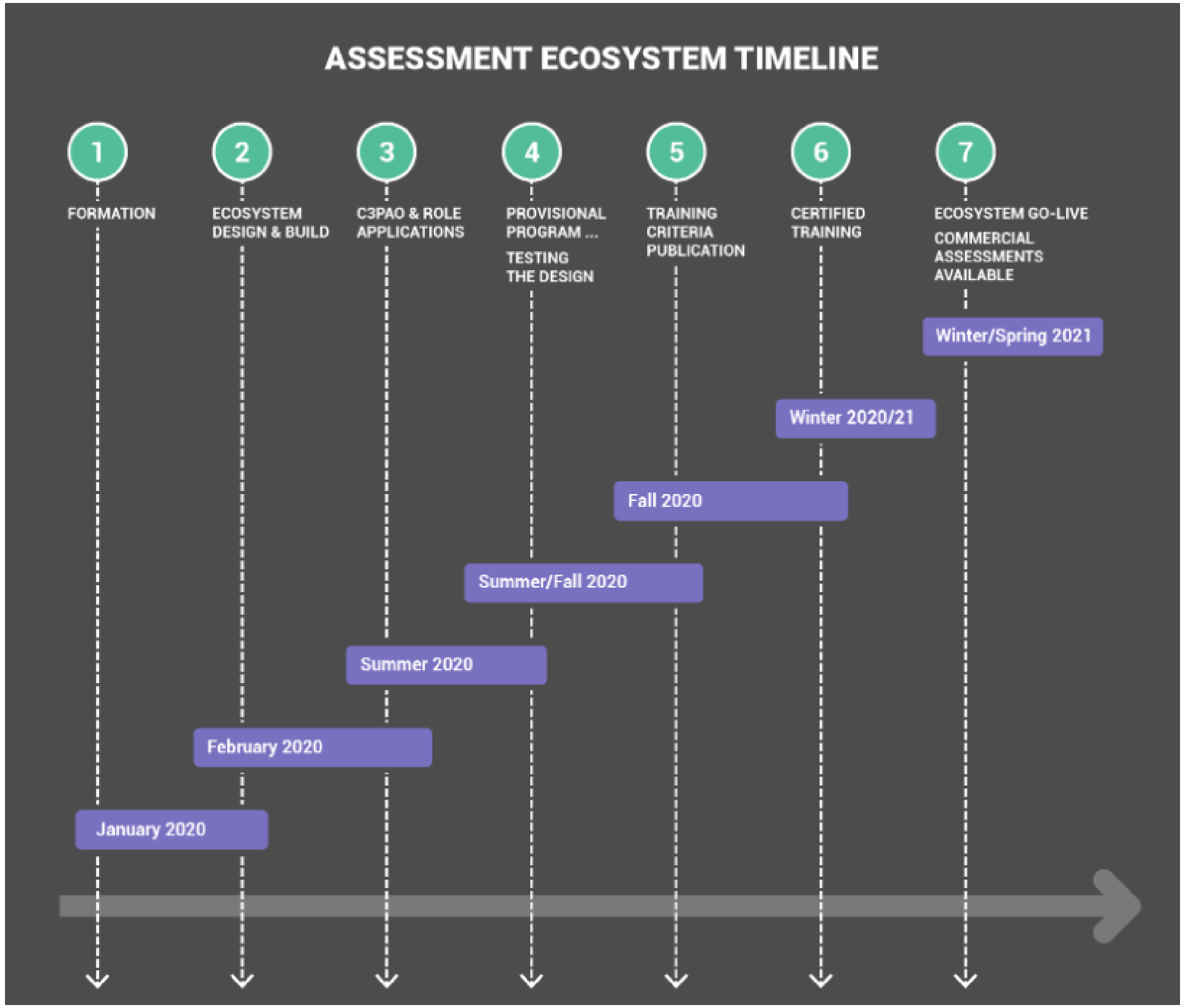
https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

Obtaining Certification

- The CMMC Accreditation Body (CMMCAB) is responsible for certifying organizations, along with those instrumental in the process (education, assessment, etc)
- Organizations must remember that this is a new process and some of the details are still being worked out in 2021
- At the time of this presentation only two Third-Party Assessor Organizations (C3PAO) have been accredited
- Many more details are still being released every month

- More specific details can be found at https://cmmcab.org/

CMMCAB Path to an Accreditation Ecosystem



https://cmmcab.org/

Roles for Cybersecurity Professionals & Organizations

Individual Professionals:

- Certified CMMC Professionals (CCP)
- Certified CMMC Assessors (CCA)
- Registered Practitioners (RP)
- CMMC-AB Certified Instructors

Organizations:

- CMMC Third-Party Assessor Organization (C3PAO)
- Registered Provider Organization (RPO)
- Organizations Seeking Certification (OSC)
- Licensed Partner Publisher (LPP)
- Licensed Training Providers (LTP)

Projected Timeline for Implementation

- The plan is for a phased rollout of CMMC between 2021-2025
- In 2021, no more than 15 Prime acquisitions will require CMMC
- But each subcontractor on those must be certified at the appropriate CMMC level
- The impacts, especially on SMBs, is still being heavily debated

- The following table represents the Prime acquisition targets for the program in coming years:

2021	2022	2023	2024	2025
15	75	250	325	475

In Summary, Actionable Next Steps

1. Organizations need to determine whether they will be responsible for being CMMC certified or not
2. Those that will need to be certified need to establish at what level they will need to be certified
3. Once a target has been set, an organization should perform a gap assessment against the appropriate level
4. Once gaps are identified, implementation plans to remediate the discovered gaps should begin immediately
5. Once all gaps are addressed, then an organization should pursue formal certification

CMMC Primary Sources – Bibliography

- https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf
- https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl1_20201208_editable.pdf
- https://www.acq.osd.mil/cmmc/docs/CMMC_AG_Lvl3_20201208_editable.pdf
- https://www.acq.osd.mil/cmmc/faq.html

- https://cmmcab.org/

- https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- https://csrc.nist.gov/publications/detail/sp/800-171a/final

RESOURCES AND CONTACT INFORMATION

JAMES TARALA

Principal Consultant at Enclave Security

James.tarala@enclavesecurity.com

RESOURCES FOR FURTHER STUDY:

SANS Webcasts

AuditScripts.com Risk Resources

SANS MGT415: A Practical Introduction to Cyber Security Risk Management

SANS SEC566: Implementing and Auditing the Critical Security Controls