



Cybersecurity Maturity Model Certification (CMMC)

CMMC Model v1.0

31 January 2020



Without a Secure Foundation All Functions are at Risk

Cost, Schedule, and Performance

are only effective in a **SECURE ENVIRONMENT**





CMMC Model v1.0 Overview

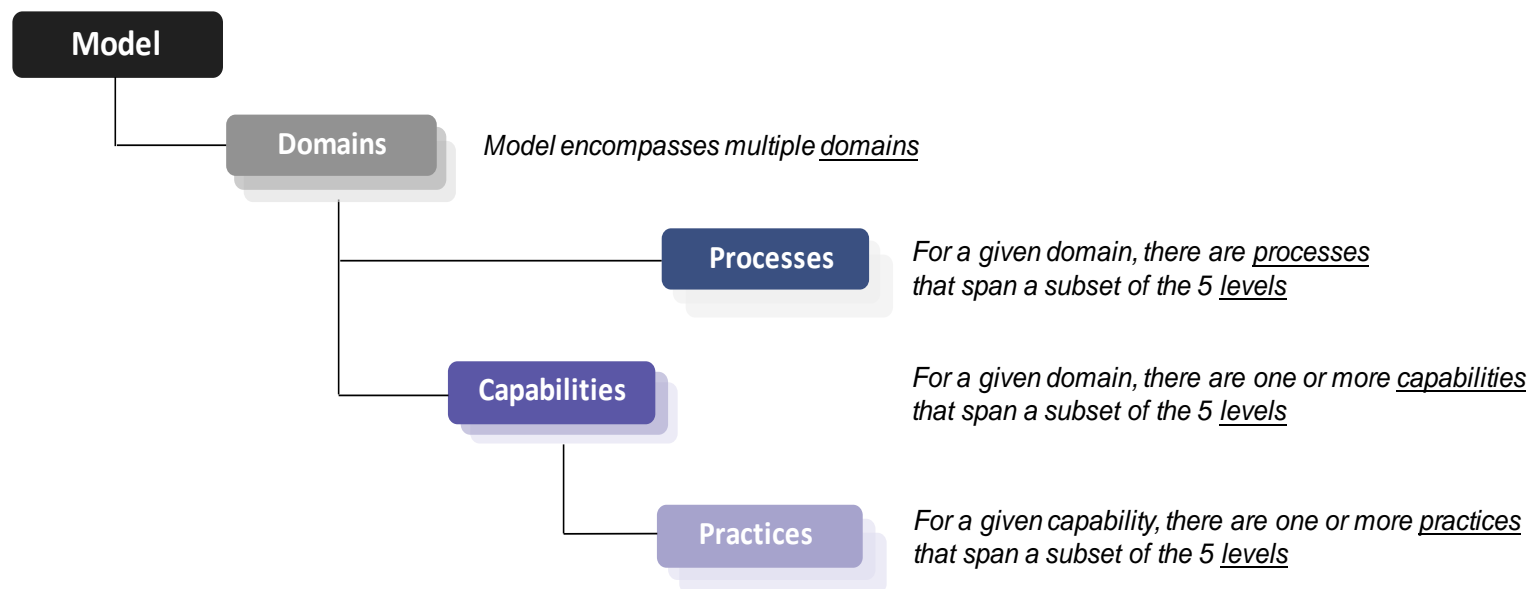
- **CMMC is a unified cybersecurity standard for future DoD acquisitions**
- **CMMC Model v1.0 encompasses the following:**
 - 17 capability domains; 43 capabilities
 - 5 processes across five levels to measure process maturity
 - 171 practices across five levels to measure technical capabilities

CMMC Model v1.0: Number of Practices and Processes Introduced at each Level

CMMC Level	Practices	Processes
Level 1	17	-
Level 2	55	2
Level 3	58	1
Level 4	26	1
Level 5	15	1



CMMC Model Framework



- **CMMC model framework organizes processes and cybersecurity best practices into a set of domains**
 - Process maturity or process institutionalization characterizes the extent to which an activity is embedded or ingrained in the operations of an organization. The more deeply ingrained an activity, the more likely it is that:
 - An organization will continue to perform the activity – including under times of stress – and
 - The outcomes will be consistent, repeatable and of high quality.
 - Practices are activities performed at each level for the domain

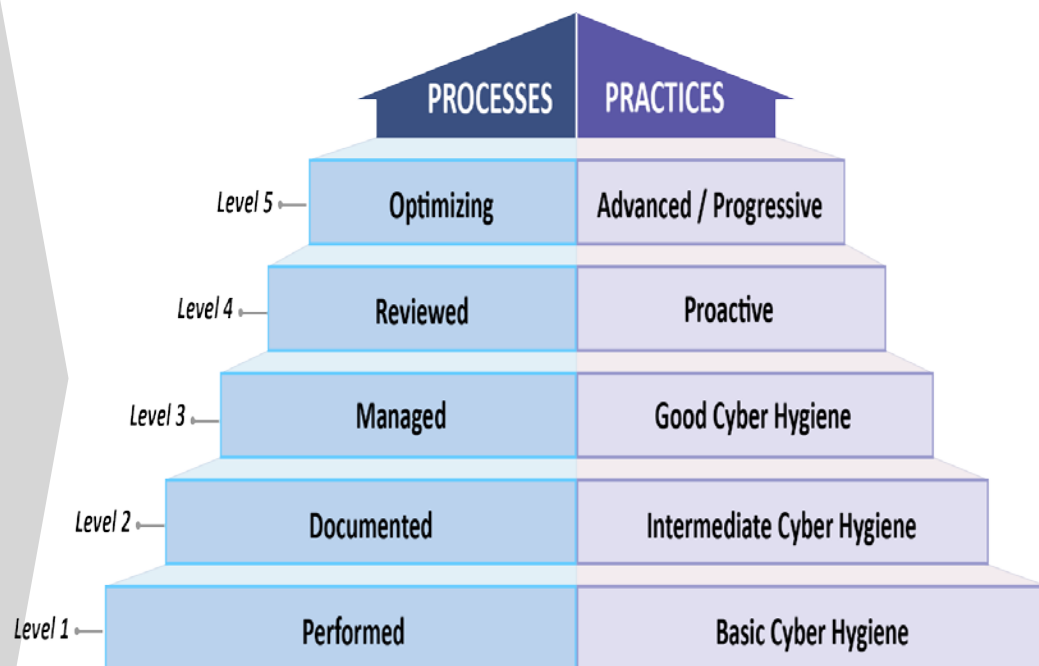


CMMC Model Structure

17 Capability Domains (v1.0)

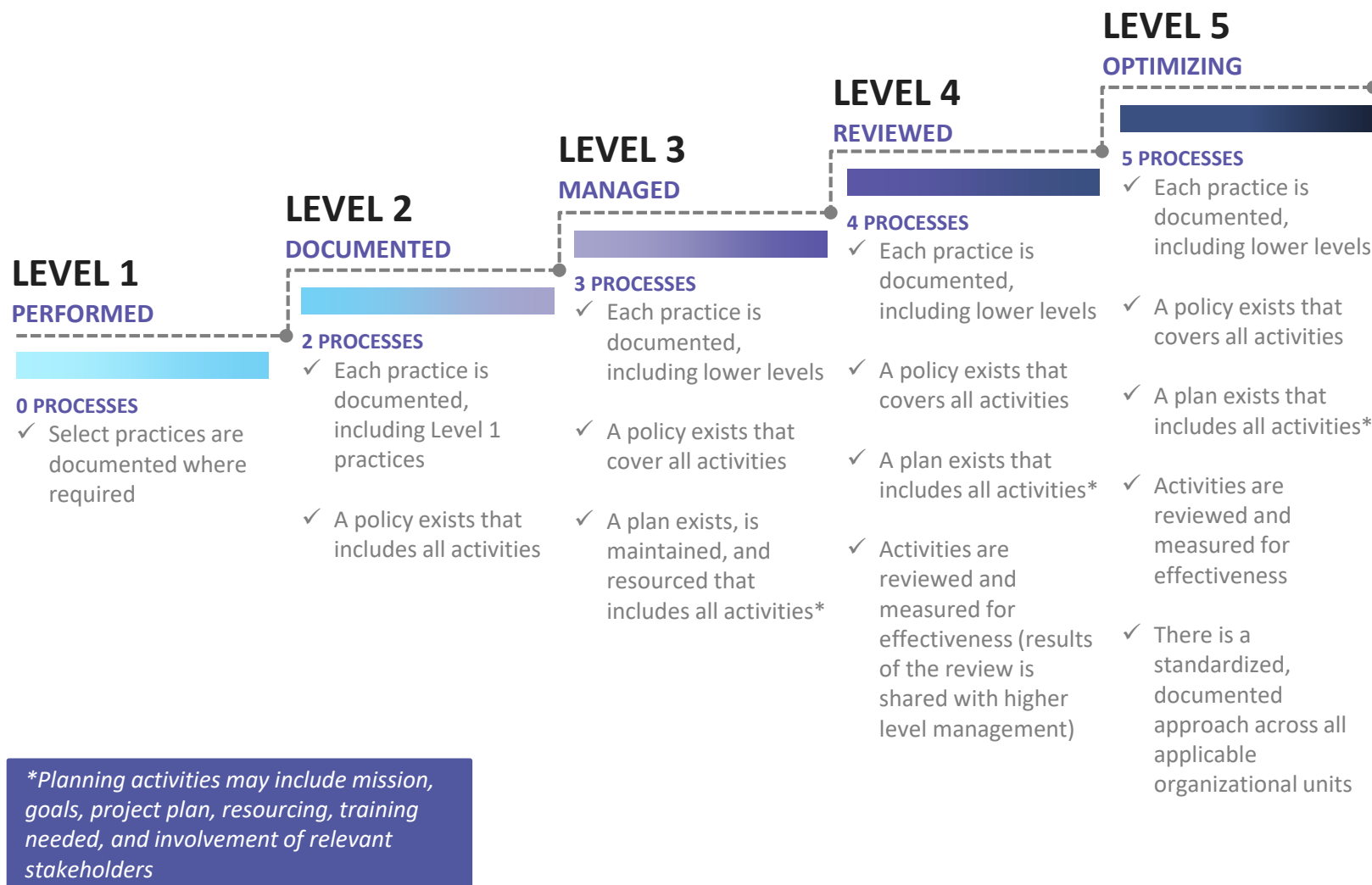
Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)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

CMMC Model with 5 levels measures cybersecurity maturity



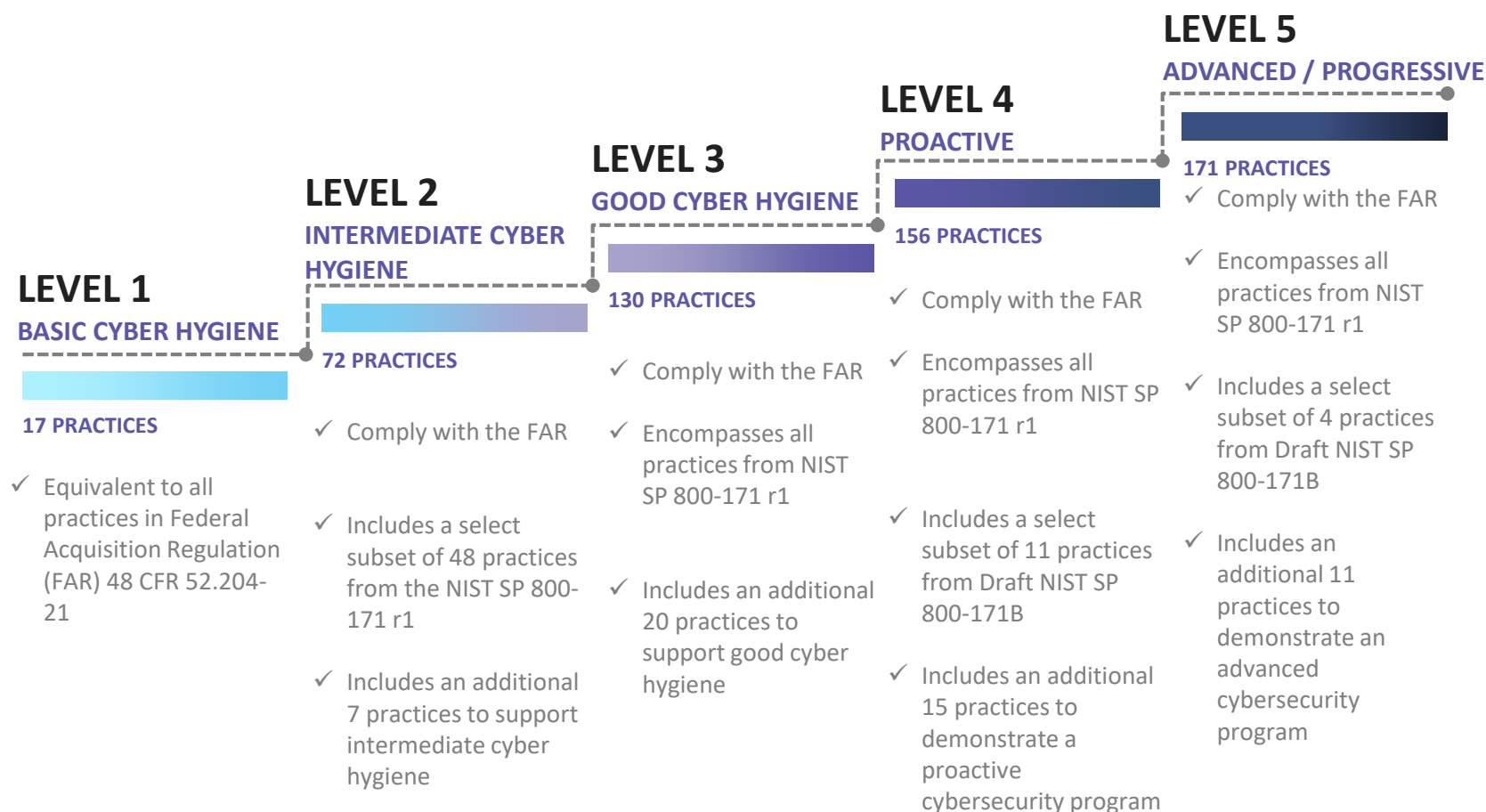


CMMC Maturity Process Progression



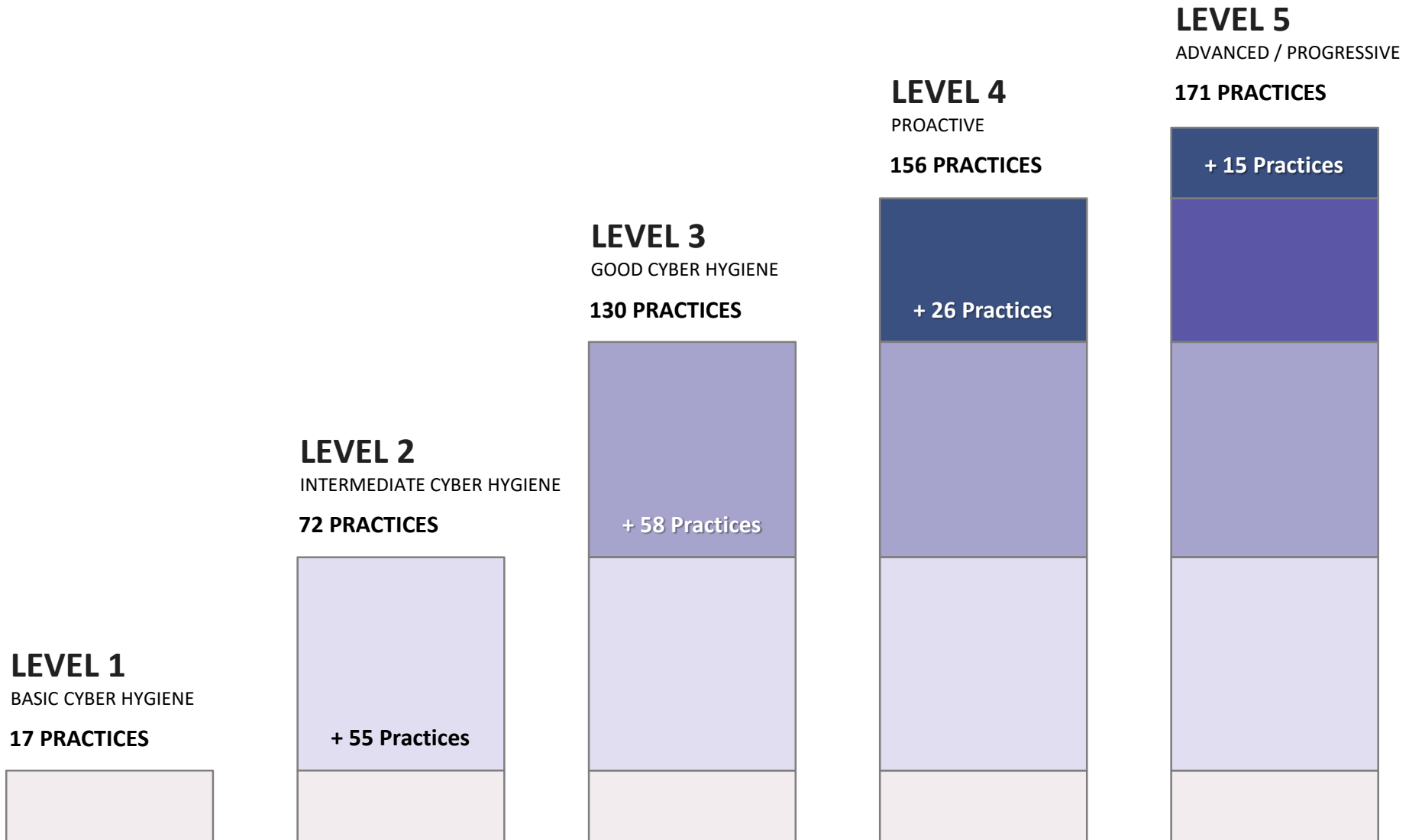


CMMC Practice Progression





CMMC Practices Per Level





CMMC Model v1.0 Source Counts

- **Model leverages multiple sources and references**

- CMMC Level 1 only addresses practices from FAR Clause 52.204-21
- CMMC Level 3 includes all of the practices from NIST SP 800-171r1 as well as others
- CMMC Levels 4 and 5 incorporate a subset of the practices from Draft NIST SP 800-171B plus others
- Additional sources, such as the UK Cyber Essentials and Australia Cyber Security Centre Essential Eight Maturity Model, were also considered and are referenced in the model

Draft CMMC Model v1.0: Number of Practices per Source

CMMC Level	Total Number Practices Introduced per CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B **	Other
Level 1	17	15*	17*	-	-
Level 2	55	-	48	-	7
Level 3	58	-	45	-	13
Level 4	26	-	-	11	15
Level 5	15	-	-	4	11

* Note: 15 safeguarding requirements from FAR clause 52.204-21 correspond to 17 security requirements from NIST SP 800-171r1, and in turn, 17 practices in CMMC

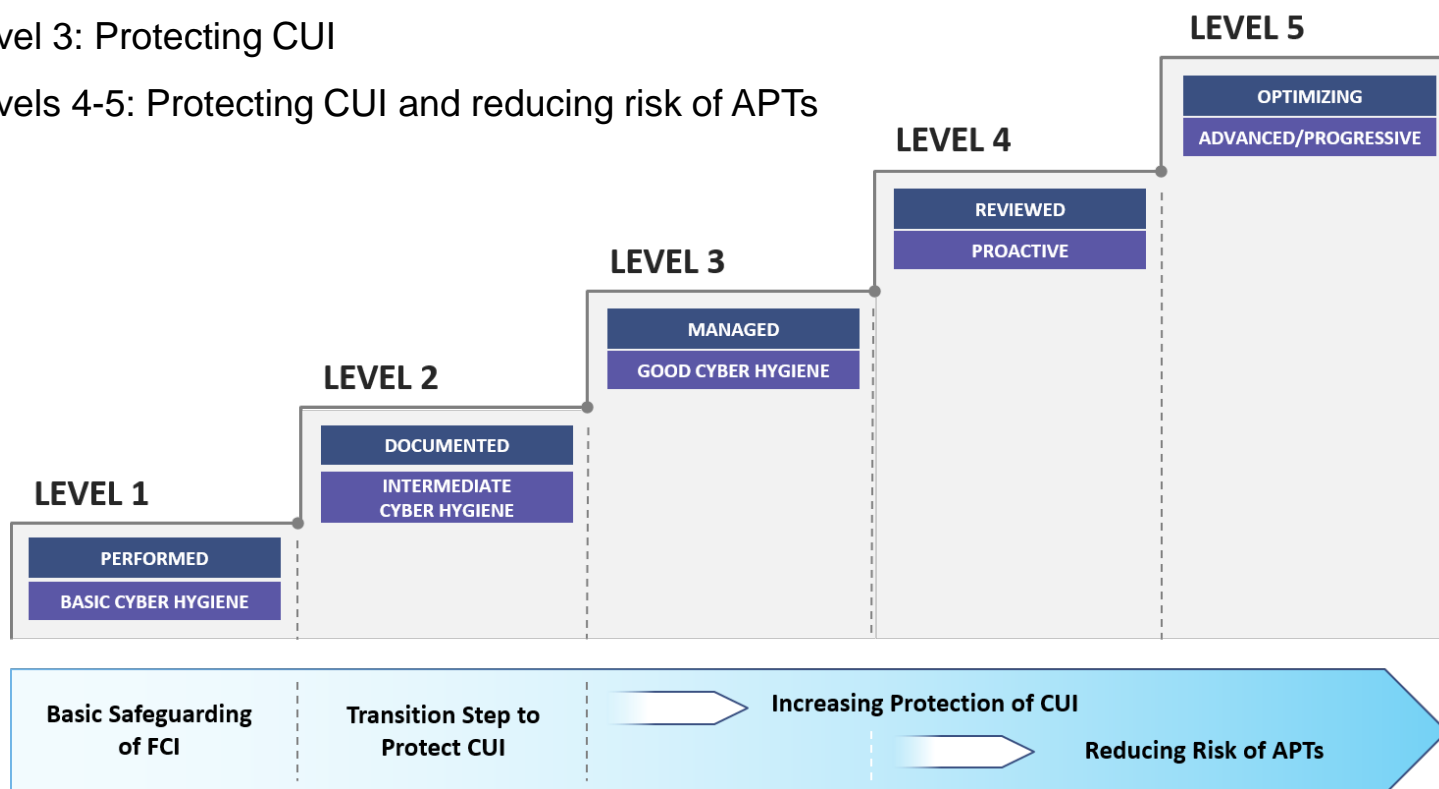
** Note: 18 enhanced security requirements from Draft NIST SP 800-171B have been excluded from CMMC Model v1.0



Summary

- **CMMC establishes cybersecurity as a foundation for future DoD acquisitions**
- **CMMC levels align with the following focus:**

- Level 1: Basic safeguarding of FCI
- Level 2: Transition step to protect CUI
- Level 3: Protecting CUI
- Levels 4-5: Protecting CUI and reducing risk of APTs





Backups





Supporting Documentation Summary



- **CMMC Model v1.0 document consists of the following:**

- Introduction, CMMC Model, and Summary
- Appendix A: CMMC Model v1.0
- Appendix B: Process and Practice Descriptions
- Appendix C: Glossary
- Appendix D: Abbreviations and Acronyms
- Appendix E: Source Mapping
- Appendix F: References



Appendix A: CMMC Model v1.0

- Appendix A provides the model in tabular form with all practices organized by Domain (DO), Capability, and Level (L)

- Practices are numbered as DO.L.###, with a unique number ###
- Each practice includes up to nine sources

- Appendix A also includes maturity level processes

- Processes are generalized but apply to all domains
- Processes are numbered as ML.L.99#

DOMAIN: ACCESS CONTROL (AC)					
CAPABILITY	Level 1 (L1)	Level 2 (L2)	PRACTICES Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C001 Establish system access requirements	AC.1.001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.3.1 • NIST SP 800-171 3.1.1 • AU ACSC Essential Right • NIST SP 800-53 AC-2, AC-3, AC-17 • NIST CSF PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CIS Controls v7 1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11 • CERT RMK v1.2 TM-SG4-SP1	AC.2.005 Provide privacy and security notices (consistent with applicable CUI rules). • NIST SP 800-171 3.1.9 • NIST SP 800-53 AC-6			
		AC.2.006 Limit use of portable storage devices on internal systems. • NIST SP 800-171 3.1.21 • NIST SP 800-53 AC-20(2) • NIST CSF BA.AM-4, PR.PT-2 • CIS Controls v7 13.7, 13.8, 13.9			
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.1.6 • NIST SP 800-171 3.1.2 • NIST SP 800-53 AC-2, AC-3, AC-17 • NIST CSF PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4 • CIS Controls v7 1.4, 1.6, 5.1, 6.5, 14.6, 15.10, 16.8, 16.9, 16.11 • CERT RMK v1.2 TM-SG4-SP1	AC.2.007 Employ the principle of least privileges (including the duties of individuals to reduce the risk of inadvertent activity without collusion). • NIST SP 800-171 3.1.5 • UK NCSC Cyber Essentials • NIST SP 800-53 AC-4, AC-6(1), AC-6(3) • NIST CSF PR.AC-4 • CIS Controls v7 14.6 • CERT RMK v1.2 KM-SG4-SP1	AC.3.017 Separate the duties of individuals to reduce the risk of inadvertent activity without collusion. • NIST SP 800-171 3.1.4 • NIST SP 800-53 AC-5 • NIST CSF PR.AC-4	AC.4.023 Control information flows between security domains on connected systems. • DMIC, modification of Draft NIST SP 800-171B 3.3.3e • NIST SP 800-53 AC-4, AC-4(1), AC-4(6), AC-4(8), AC-4(12), AC-4(13), AC-4(15), AC-4(20), SC-40 • NIST CSF BA.AM-3, PR.AC-5, PR.DS-5, PR.PT-4, HE.AE-1 • CIS Controls v7 12.1, 12.2, 13.1, 13.3, 14.1, 14.2, 14.5, 14.6, 14.7, 15.6, 15.10	AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • DMIC • NIST SP 800-53 SC-41(4) • NIST CSF PR.DS-5, HE.AE-1, DE.CM-7 • CIS Controls v7 15.3
		AC.2.008 Use non-privileged accounts or roles when accessing information functions. • NIST SP 800-171 3.1.6 • UK NCSC Cyber Essentials • NIST SP 800-53 AC-4(2) • NIST CSF PR.AC-4 • CIS Controls v7 4.3, 4.6	AC.3.018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 3.1.7 • NIST SP 800-53 AC-4(9), AC-4(10) • NIST CSF PR.AC-4 • CERT RMK v1.2 KM-SG4-SP1	AC.4.025 Periodically review and update CUI program access permissions. • DMIC	

Appendix A Practices

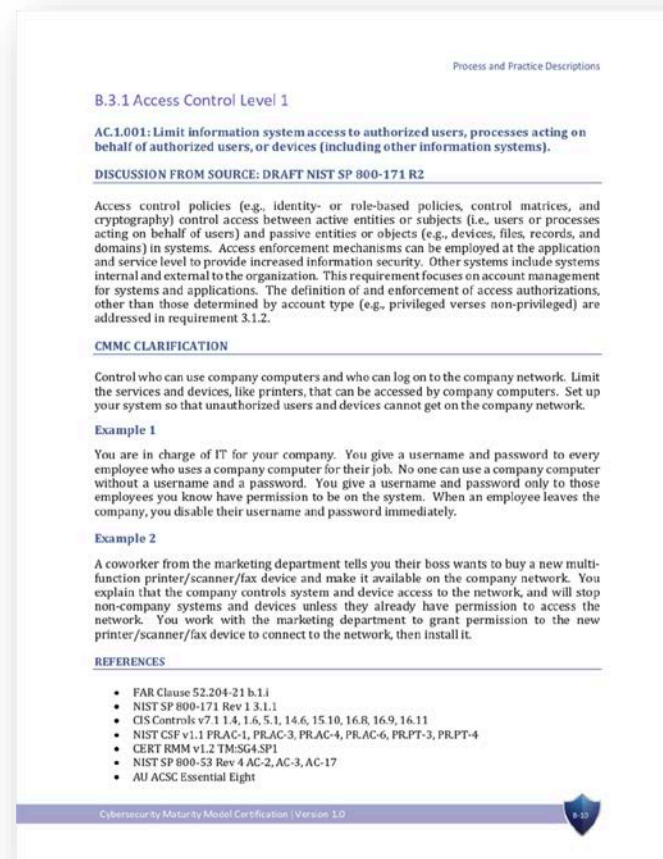
PROCESS MATURITY (ML)					
MATURITY CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
ML01 Improve [DOMAIN NAME] activities	ML2.099 Establish a policy that includes [DOMAIN NAME] • CERT RMK v1.2 GIG-GP1 subjective 2	ML3.097 Establish, maintain, and resource a plan that includes [DOMAIN NAME] • CERT RMK v1.2 GIG-GP2	ML4.096 Review and measure [DOMAIN NAME] activities for effectiveness. • CERT RMK v1.2 GIG-GP8	ML5.095 Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organizational units. • CERT RMK v1.2 GIG-GP1	
	ML2.098 Establish practices to implement the [DOMAIN NAME] policy. • CERT RMK v1.2 GIG-GP2 subjective 2				

Appendix A Processes



Appendix B: Process and Practice Descriptions

- **Appendix B Process and Practice Descriptions include:**
 - Discussion, derived from source material where available
 - Clarification with examples
 - A list of references
- **Same framework as model**
 - Processes are generalized but apply to all domains
 - Practices are ordered by domain and level



Appendix B Practice & Process Descriptions



Appendix E: Source Mapping

- **Appendix E Source Mapping summarizes the list of sources for all five processes and 171 practices**
- **Sources include:**
 - FAR Clause 52.204-21
 - NIST SP 800-171 Rev 1
 - Draft NIST SP 800-171B
 - CIS Controls v7.1
 - NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1
 - CERT Resilience Management Model (CERT RMM) v1.2
 - NIST SP 800-53 Rev 4
 - Others such as CMMC, UK NCSC Cyber Essentials, or AU ACSC Essential Eight

Source Mapping

Appendix E. Source Mapping

This source mapping provides a detailed list of related practices from other frameworks corresponding to each CMMC practice. In this way, the mapping allows an organization to easily identify which CMMC practices correspond to sources in other frameworks that the organization may already be using or may need to reference in the future.

The CMMC practices that align with the FAR Clause 52.204-21 and NIST SP 800-171 Rev 1 are identical to the reference practices. An organization that meets the requirements for the CMMC practice will also meet the requirements for these security requirements. The additional sources are for reference only and do not guarantee that if an organization meets the requirements of these additional sources they will also meet the corresponding CMMC practice. Some practices are sourced to "CMMC" to indicate that they were developed by the CMMC working team or through collaboration with industry.

The below table summarizes related sources for each CMMC practice.

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 1	DRAFT NIST SP 800-171B	CIS Controls v7.1	NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF) v1.1	CERT Resilience Management Model (CERT RMM) v1.2	NIST SP 800-53 Rev 4	Other
Process Maturity	ML.2.099						GG2 GP1 subpractice 2		
	ML.2.098						GG2 GP2 subpractice 2		
	ML.3.097						GG2 GP2 subpractice 2		
	ML.4.096						GG2 GP3		
	ML.5.095						GG2 GP8		
	ML.5.095						GG3 GP1, GG3 GP2		
Access Control	AC.1.001	9.1.i	3.1.1		1.4, 1.6, 3.1, 3.4, 15.10, 16.8, 16.9, 16.11	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.AC-7, PR.AC-8	TM-SGA-SP1	AC-2, AC-3, AC-17	AU ACSC Essential Eight
	AC.1.002	9.1.ii	3.1.2		1.4, 1.6, 3.1, 3.4, 14.6, 15.10, 16.8, 16.9, 16.11	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.AC-7, PR.AC-8	TM-SGA-SP1	AC-2, AC-3, AC-17	
	AC.1.003	9.1.iii	3.1.20		12.1, 12.4	ID.AMA-4, PR.AC-9	IXD-SG1-SP1	AC-20, AC-20(1)	
	AC.1.004	9.1.iv	3.1.22					AC-22	
	AC.1.005		3.1.9					AC-8	

Cybersecurity Maturity Model Certification | Version 1.0

Appendix E Source Mapping