





Cybersecurity Maturity Model Certification (CMMC)

CMMC Model v1.0

31 January 2020



Without a Secure Foundation All Functions are at Risk









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

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



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)

CMMC Model with 5 levels measures cybersecurity maturity









*Planning activities may include mission, goals, project plan, resourcing, training needed, and involvement of relevant stakeholders

DISTRIBUTION A. Approved for public release

organizational units

















• 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

СММС	Total Number Practices		Soι	irce	
Level	Introduced per CMMC Level	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

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

* 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



OPTIMIZING













• 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 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#

CAPABILITY			PRACTICES		
CAPABILITY	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C091 Extablish system access requirements	ACLIOT LURI identification system access to authorized sures, processes acting one head of authorized sures, or devices thead of authorized sures, or devices thead of authorized sures, or devices resolution and action action action resolution action action action resolution action	AC2005 Provide privacy and security notices consistent with applicable CCF niles. •NIST SP 800-53 AC-8 •NIST SP 800-53 AC-8			
		AC 2006 Limit use of portable storage devices on external systems. NIST 59 100-57 AC 20(2) - NIST 59 100-55 AC 20(2) - NIST 65 F DA AL, PR.PT-2 - GE Gostrolo VI 37, 713A, 13.9			
0002	AC1.002	AC 2.097	AC3.017	AC4023	AC5.024
Control laternal system access	Limit information system access to the types of transactions and functions that authorized uners are permitted to esocials. • FAR Clausie 52:204-21 h.1.8 • NIST SF 800-171.3.1.2 • NIST SF 800-53.4.C.2, A.C.4, AC-17	Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST 59: 800-1713.1.5 • UIX NSC 6(yet Essentials • NIST 59: 800-53: AC-6, AC-6(1), AC- 0(5) • NIST CSF PRAC-4 • CIS Controls VI 146	Separate the duties of individuals to	Control Information Blook Detween security domains on consented systems. • CMMC molification of Draft NIST SP 800-57183.3.a • SINTE SP 100-58 AC-4, 40, AC-4, 41, AC- 4, 40, AC-4, 41, AC-4, A	Memting and mitigate risk associated with workertified wireless access point entencied to the metwork. COMMC = NISTS 97 HIDO 53 SE-4 (14) = NISTS 97 HIDO 53 SE-4 (14) = NISTS 97 HIDO 53 SE-4 (14) = CIS Generative 7153
		AC 2.008 Use non-provideged accounts or roles when accessing nonsecurity functions. • NIST 52 800-173.2.1.6 • VR NIST 52 800-53 AC 4(2) • NIST 52 800-53 AC 4(2) • NIST 55 PLAC-4 • CIS Controls v7 4.3.4.6	AC3.019 Prevent noi-privileged users from executing privileged functions and conterve the encountion of such functions in auda logs. • NIST SP 8060-171 3.1.7 • NIST SP 8060-324 Co(91, AC-6(10) • NIST SP 80-53 AC-6(91, AC-6(10) • NIST SP 80-53 AC-6(91, AC-6(10)) • NIST SP 80-53 AC-6(91, AC-6(10))	AC4.025 Periodically review and update CJI program acress permissions. • CMMC	

Appendix A Practices

MATURITY CAPABILITY			PROCESSES		
MATORITY CAPABILITY	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
MCO1 Improve [DOMAIN NAME] activities		ML2.999 Bitzbish a policy that includes [DOMAIN NAME]. • CERT RMM v1.2 GG2.GP1 subpractice 2		ML 4.996 Review and measure [EOMAIN NAME] activities for effectiveness. • CERT RMM v1.2 GG2.GP0	ML5.995 Standardize and optimize a documented approach for [DOMAIN XAME] accord all applicable organizational units. • CIRT RMM v1.2 GGLCP1
		ML2.998 Establish practices to implement the [DOMAIN NAME] policy. - CERT RIMM v1.2 GG2.GP2 subpractice 2			

Appendix A Processes



Appendix B: Process and Practice Descriptions



ocess 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

222222222	
DISCUSSI	ION FROM SOURCE: DRAFT NIST SP 800-171 R2
cryptogra acting on domains) and servic internal a for systen other that	ontrol policies (e.g., identity- or role-based policies, control matrices, and phy) control access between active entities or subjects (i.e., users or processes behalf of users) and passive entities or objects (e.g., devices, files, records, and in systems. Access enforcement mechanisms can be employed at the application celevel to provide increased information security. Other systems include systems and external to the organization. This requirement focuses on account management ms and applications. The definition of and enforcement of access authorizations, in those determined by account type (e.g., privileged verses non-privileged) are d in requirement 3.1.2.
CMMC CL	ARIFICATION
the servic	ho can use company computers and who can log on to the company network. Limit es and devices, like printers, that can be accessed by company computers. Set up em so that unauthorized users and devices cannot get on the company network.
Example	1
employee without a employee	n charge of IT for your company. You give a username and password to every who uses a company computer for their job. No one can use a company computer to their job. No one can use a company computer susername and a password. You give a username and password only to those so you know have permission to be on the system. When an employee leaves the you disable their username and password immediately.
Example	2
function p explain th non-comp network.	er from the marketing department tells you their boss wants to buy a new multi- printer/scanner/fax device and make it available on the company network. You ta the company control's system and device access to the network, and will stop pany systems and devices unless they already have permission to access the You work with the marketing department to grant permission to the new canner/fax device to connect to the network, then install it.
REFERENC	CES
 NIS CIS NIS CEI NIS 	R Clause 52:204-21 b.1.1 ST SP 800-171 Rev 1 3.1.1 St CSF v1.1 PR.Ac.4, pr.Ac.6, 15 10, 16.8, 16.9, 16.11 ST CSF v1.1 PR.Ac.4, pr.Ac.6, 3, PR.AC6, PR.PT-3, PR.PT-4 RT RMM v1.2 TM:SG4.SP1 ST SP 800-53 Rev 4 AC-2, AC-3, AC-17 ACSC Essential Eight
Cybersecur	rty Maturity Model Certification (Version 1.0

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

Appendix E. Source Mapping This source mapping provides a detailed lis corresponding to each CMMC practice. In the saily identify which CMMC practices corress regulazion may already be using or may ne the CMMC practices that align with the FAR are identical to the reference practices. An or CMMC practice will also meet the require reductional sources are for reference only and he requirements of these additional sources practice. Some practices are sourced to "CMM CMMC working team or through collaboration The below table summarizes related sources the source of the source of the source of the sources the source of the source of the source of the sources the source of the source of the source of the sources the source of the source of the source of the sources the source of the source of the source of the sources the source of the source of the source of the source of the sources the source of the source of	t of rel is way, pond to ed to re Clause ganizat ments f do not s they w 4C* to ir n with i	the mappi sources i ference in 52.204-21 ion that m for these s guarantee rill also me idicate tha ndustry.	ng allows in other fra the future and NIST eets the re- security re that if an o- tet the cor t they were actice.	an organi mework: SP 800-1 quiremen quiremen rganizati respondi e develop	71 Rev 1 ts for the ts for the nts. The on meets ng CMMC
Conception of the second secon	is way, pond to ed to re Clause rganizat ments f do not s they w 4C* to in n with i for eacl	the mapping sources in ference in 52.204-21 ion that may for these as guarantee vill also me adicate that ndustry. h CMMC proving Creation for inproving Creation to reprove the creation of the construction constr	ng allows in other fra the future and NIST eets the resecutivy re that if an o tet the corr actice.	an organi mework: SP 800-1 quiremen quiremen rganizati respondi e develop	71 Rev 1 ts for the ts for the nts. The on meets ng CMMC
CIMC practice will also meet the require MMC practice will also meet the require additional sources are for reference only and the requirements of these additional sources are sourced to "CMN ZMMC working team or through collaboratio The below table summarizes related sources Contact FAR Practice CAR FAR Fraction Contact Sources Contact FAR Practice Care NST92 800 DALFT NST Domain ML 2009 DISC DALFT NST ML 200	ganizat ments f do not s they w dC* to in n with i for each	ion that m for these s guarantee rill also me ndicate tha ndustry. h CMMC pr NeST Framework for Improving Critical Infrastructure Cyberneourky	eets the reisecurity reithat if an eithat if an eithe continue they were actice.	quiremen quireme rganizati respondi e develop NST SP 100-33 Key	ts for the nts. The on meets ng CMMC
CHANC EAR Practice Clever NoT 99 800 DRAFT NOT Domain No. 2 306 21 071 Rev 1 09 806 1718 ML 2.998 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	CIS Controls	NIST Framework for improving Critical Infrastructure Cybersecurity	CERT Resilience Management Model (CERT-	800-53 Rev	
Practice Classe NST 59 800. DRAFT NST Dovesin 10 52 200-21 171 8w 1 99 800.1718 ML2.1999 ML2.2098 ALL ST	Controls	Framework for improving Critical Infrastructure Cyberneourity	Resilience Management Model (CERT-	800-53 Rev	
ML 2.999 ML 2.998					Other
Design Manufacture			GG2.GP1 subpractice 2		-
Process Maturity ML 3.997			662.6P2		
		1	subpractice 2 GG2.GP2.		
ML 4.096			GG2.GP3 GG2.GP8	-	
ML5.995			663.6P1, 663.6P2		
AC.1001 53/ 313	1.4, 1.6, 5.1, 14.6, 15.10, 16.8, 16.9, 16.11	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4	TM:SG4.9P1	AC-2, AC-3, AC-17	AU ACSC Essential Eight
Access Cambrol Ac.1.002 b.1.8 3.1.2	1.4, 1.6, 5.1, 8.5, 14.6, 15.10, 16.8, 16.9, 16.11	PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-6, PR.PT-3, PR.PT-4	TM:SG4.SP1	AC 2, AC 3, AC 17	
AC.1.003 9-1.# 3.1.20	12.1, 12.4	ID AM-4, PR.AC-3	EXD563.5P1	AC-20, AC-20(1)	
AC.1.004 0.1.iv 3.1.22				AC-22	1
AC.2.005 3.1.6				AC-8	