Preliminary Analysis of CMMC v0.7

A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) v0.7 Soliciting Input and Comments

Analysis and comments on the CMMC v0.7 are provided. The analysis and discussion are short and to the point. CMMC is nearing finalization and changes are small. The statistics of domains, capabilities, practices, and processes is provided and compared to other standards.

Abstract

Michael G. Semmens
President & CEO, Imprimis Inc.
Chairman, National Cyber Exchange

Steve Lines
Executive Director of Cyber Technology & ISAO Operations
National Cyber Exchange

Jennifer Kurtz
Cyber Program Director
Manufacturer's EDGE

BLUF (Bottom Line Up Front)

The CMMC v0.7 adds a number of practices at levels 4 and 5 which are largely informed by NIST SP 800-171B, the derivative NIST 800-171 standard with enhanced requirements for increased security. Very little change was made to levels 1-3, moving 3 practices from level 2 to level 3. Two additional capabilities were added in support of levels 4 and 5. It is clear that the size and content have been shaped to make primary use of NIST SP 800-171 at level 3 and NIST SP 800-171B for levels 4 and 5 as promised by OSD. Key takeaways from v0.7 are:

1. Levels 1-3 are largely unchanged with only 3 practices moved from level 2 to level 3, and other minor changes.
2. Level 4 now has 26 practices and level 5 has 43 practices and 2 capabilities were added to support the two top levels.
3. OSD is nearing the final version.

As we said in the previous paper (Reference 2), the CMMC does not represent a huge change from NIST SP 800-171 but does add some important practices that do bring value to the security baseline. However, the categories of work by level has not yet been defined. It still appears that level 3 is the first meaningful certification level.

There are many questions being asked about certification and the schedule thereof. OSD is actively developing the certification program and details should be available soon. Many are asking when they might be certified and what to do until they are officially certified. The answer is straight forward, the DFARS is still in effect and defense contractors need to protect CUI by implementing the requirements of NIST 800-171 and have a good System Security Plan (SSP) and Plan of Action and Milestones (POA&M) if one is needed. These will be the cyber currency until the full CMMC program is fully rolled out and in full effect. Clearly, DoD contracting companies, knowing that CMMC will happen soon, should work on implementing the NIST SP 800-171 security requirements – this act is important and will not be wasted effort. In fact, if an organization has NIST800-171 implemented, they are at least 84% of the way to CMMC Level 3.

Let us know what you think. Submit comments at https://nationalcyber.org/cmmc-comment-form. The three (3) CMMC papers are available here: https://nationalcyber.org/CMMC .

Preliminary Analysis of CMMC v0.7

A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) for Submittal

This paper builds on the analysis performed in the previous effort, which analyzed the CMMC v0.4 and v0.6. These paper (Reference 1 and 2) can be obtained at https://natioanlcyber.org/CMMC. It summarizes the impetus for CMMC and provides a detailed analysis of the practices, processes, and RCIs (Referenced Compliance Items) contained in version 0.7.

This paper will be by far the shortest of the three. There is simply not much new material contained in CMMC v0.7. OSD does indeed appear to be closing in on the final version.

CMMC PRACTICES, PROCESSES, AND REFERENCED COMPLIANCE ITEMS

The number of practices contained within each maturity level of CMMC is shown in Figures 1 and 2 below, and show the change from the first to last version. Very little change occurred in the first 3 levels between the v0.6 and v0.7 after seeing a very dramatic reduction from v0.4 to v0.6. Information regarding levels 4 and 5 have been only recently published.

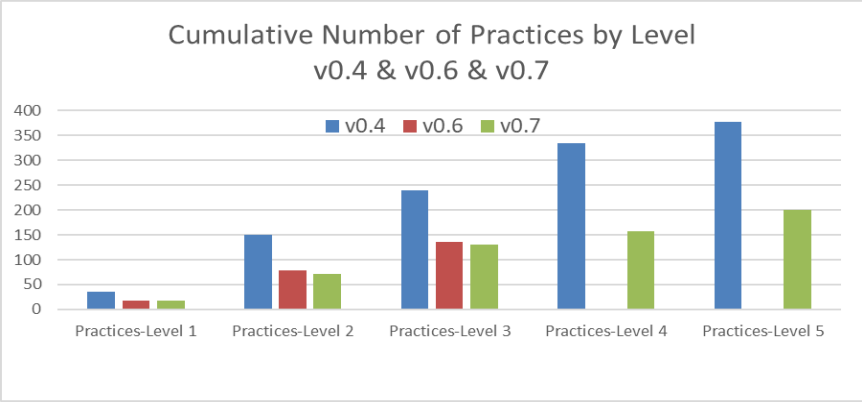

Figure 1 Number of Practices by Level and Version

The number of referenced compliance items or RCIs follows a similar pattern with a dramatic reduction after v0.4 and then modest changes after. Figure 2 shows the number of RCIs by version. As a reminder, OSD clarified that these items are not compliance requirements under CMMC but rather informed the practices that are contained within CMMC.

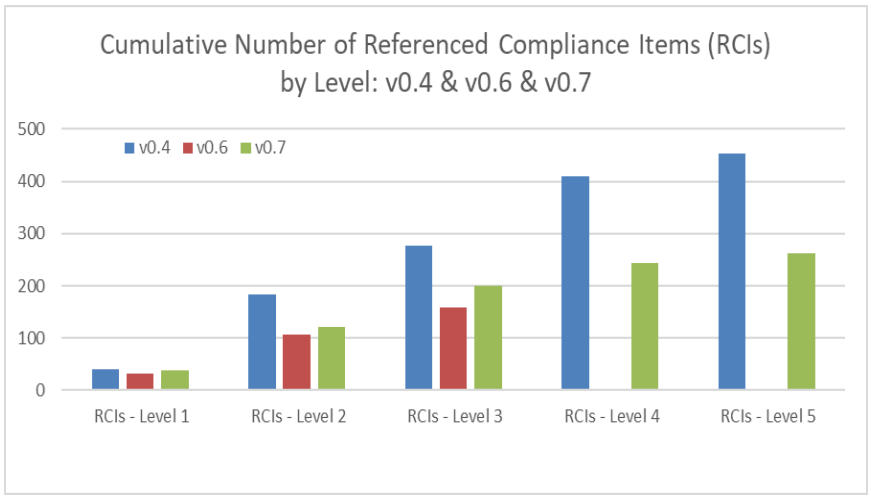

Figure 2 Number of RCIs by Level and by Version

The total count of practices, processes, capabilities, and domains is provided in Figure 3. As can be seen in this figure, the cumulative

	CMMC Domains	Capabilities Total	LEVEL 1		LEVEL 2		LEVEL 3		LEVEL 4		LEVEL 5		TOTALS	
			Practices	RCIs	Practices	RCIs	Practices	RCIs	Practices	RCIs	Practices	RCIs	Practices Total	RCI Total
1	Acces Control (AC)	4	4	5	10	13	8	9	3	3	4	1	29	31
2	Asset Management (AM)	2	0	3	0	0	2	4	1	1	2	0	5	8
3	Audit & Accountability (AA)	4	0	3	4	5	7	9	2	2	4	1	17	20
4	Awareness & Training (AT)	2	0	0	2	4	1	1	2	2	2	0	7	7
5	Configuration Management (CM)	2	0	3	6	11	3	6	1	4	2	1	12	25
6	Cybersecurity Governance (CG)													
7	ID & Authorization (IDA)	1	2	2	5	6	4	5	0	0	1	1	12	14
8	Incident Response (IR)	5	0	3	5	5	2	2	2	2	5	5	14	17
9	Maintenance (MA)	1	0	2	4	5	2	2	0	0	1	0	7	9
10	Media Protection (MP)	4	1	1	3	6	4	5	0	0	4	0	12	12
11	Personnel Security (PS)	2	0	2	2	4	0	0	0	0	2	0	4	6
12	Physical Protection (PP)	1	4	5	1	2	1	1	0	0	1	0	7	8
13	Recovery (RE)	2	0	0	2	7	1	3	0	0	2	2	5	12
14	Risk Management (RM)	3	0	0	3	5	3	6	4	6	3	3	13	20
15	Security Assessment (SAS)	3	0	1	3	3	2	2	3	7	3	0	11	13
16	Situational Awareness (SA)	1	0	2	0	0	1	1	2	10	1	0	4	13
17	System & Comms Protection (SCP)	2	2	2	2	4	15	18	5	7	2	3	26	34
18	System & Info. Integrity (SII)	4	4	4	3	4	3	3	1	1	4	2	15	14
	Practices & Controls TOTALS	43	17	38	55	84	59	77	26	45	43	19	200	263
	Maturity Processes TOTALS		0		3		2		2		2		9	
	Practices & Maturity Processes ACCUMULATIVE TOTALS	43	17		75		136		164		209			

Figure 3 Total Count of Domains, Capabilities, Practices, and Processes by Level for v0.7

number of practices reaches 200 by level 5 and is 136 at level 3 which includes 131 practices and 5 maturity processes.

There remain 17 domains as Cybersecurity Governance was removed and Policy and Governance are now addressed in the maturity processes. A total of 43 capabilities are included in the 17 domains.

The standards and controls/requirements cited throughout the CMMC are shown in Figure 4 which shows that the dominant standards that informed the CMMC are NIST800-171 and NIST800-

Figure 4 Referenced Compliance Items Cited by Level

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
FAR	15				
NIST 800-171	17	48	45	2 [2]	
NIST 800-171B				11 [3]	6 [3]
RMM	1	18	6		1
ISO 27001:2013	0	1	3		2
CSF	1	3	0	16	
CIS	1	3	8	5	2
UK NCSC	3	7	4		
AU ACSC	2	2	3		
CMMC [1]			8	11	8
TOTALS	25	82	77	32	13

Note 1: The CMMC was referenced numerous times but without specific citing of a control or practice. It was therefore not possible to provide a count of controls or practices but rather the total number of CMMC citings is shown.
Note 2: These are NIST SP 800-171 requirements modified by CMMC.
Note 3: Author's count at variance with published figures. (Shaded cells)

171B. The cumulative number of RCIs citations is shown in Figure 5 which also indicates the percentages

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	TOTAL	% OF TOTAL
FAR	15	15	15	15	15	15	6%
NIST 800-171	17	65	110	110	110	110	45%
NIST 800-171B	0	0	0	11	17	17	7%
RMM	1	19	25	25	26	26	11%
ISO 27001:2013	0	1	4	4	6	6	2%
CSF	1	4	4	20	20	20	8%
CIS	1	4	12	17	19	19	8%
UK NCSC	3	10	14	14	14	14	6%
AU ACSC	2	4	7	7	7	7	3%
CMMC (1)	0	0	8	19	27	27	11%
TOTALS	25	107	184	227	246	246	100%

Figure 5 Cumulative Number of Requirements or Controls Cited by CMMC

for each standard.

Finally, the comparison of CMMC to other standards shown in Figure 6 shows that the CMMC levels fall into a natural grouping with other like standards such as ISO 27000, NIST800-171, and the lower levels of FIPS and CNSSI 1253.

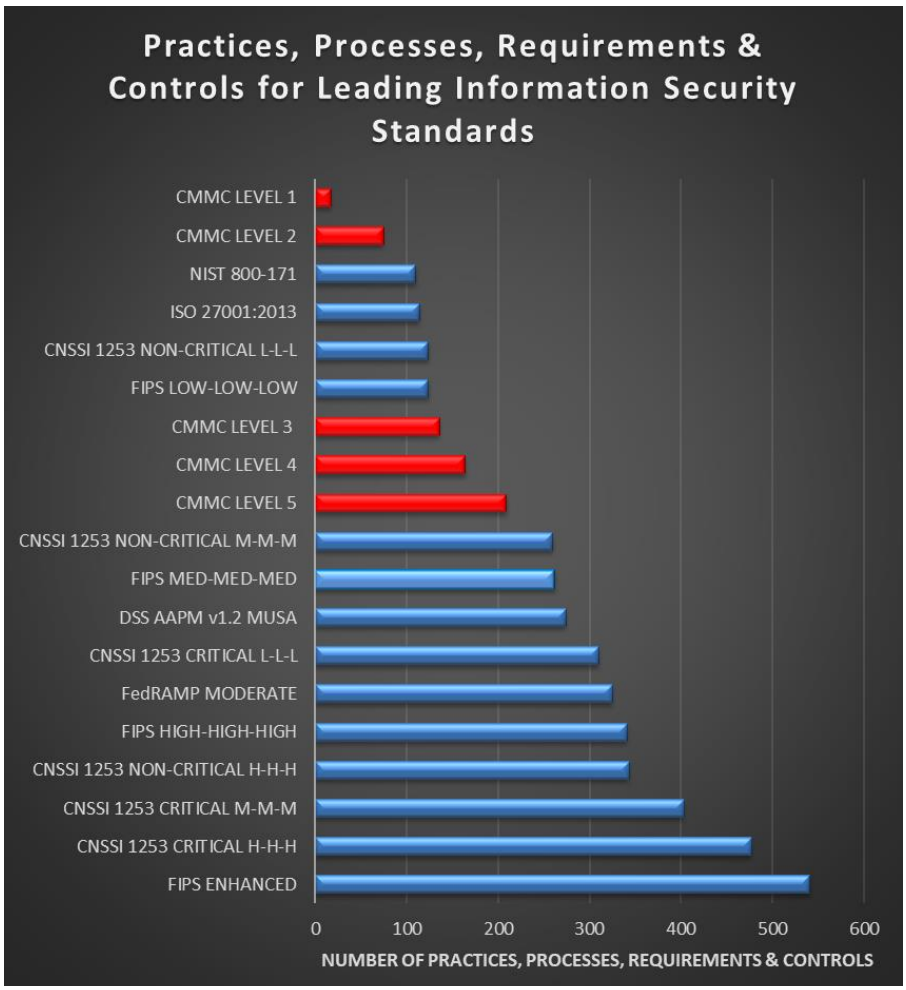

Figure 6 Comparison of CMMC to other Cybersecurity Standards

SUMMARY

This goose is cooked. The content of the CMMC is stable and does indeed reflect OSD's promise to stay close to the NIST800-171 through level 3 and the NIST800-171B for levels 4 and 5. CMMC will continue to evolve, the initial version – v1.0 is due out in January or later this month. It is very unlikely to change much, if at all.

So, attention is now turned to the remaining questions; the level of maturity required to do specific categories of work, and how/when to get certified.

With regard to determining the work to be performed at each level of maturity, the consensus is that Level 3 will be the minimum level for any work that involves sensitive data or CUI. This was mentioned in previous papers. CMMC references the AIA NAS 9933 standard, and AIA makes it clear that it requires level 3 for important work. The guidance provided in the DoD briefings indicates that level 3 will provide only "*moderate resistance against data exfiltration,"* and level 2 states that it provides only *"minor resistance to data exfiltration."* These definitions might be interpreted in a way that indicates level 4 is the first acceptable level. However, speculation is that level 3 is the first meaningful level.

Certification is the long pole in the tent. OSD is actively searching for a non-profit to act as the certifying agency, but that will take a while. They then must determine the process, find and train the auditors and then start the certification of many contractors – possibly as many as 300,000. This too will take some time. In the meantime, all efforts should be put into the implementation of the NIST800-171 requirements and maintaining a solid SSP and POA&M, if needed.

Let us know what you think. Submit comments to https://nationalcyber.org/CMMC and the DIB ISAC, and the NCX will make sure all comments are received by the CMMC team.

References

1. Preliminary Analysis of CMMC v0.6, A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) v0.6 Soliciting Input and Comments, M.G. Semmens, J. Kurtz, S. Lines, December 2019.
2. Preliminary Analysis of CMMC v0.4, A Green Paper: Analysis of The DoD Cybersecurity Maturity Model Certification (CMMC) v0.4 Soliciting Input and Comments, M.G. Semmens, J. Kurtz, S. Lines, November 2019.
3. *'Cybersecurity Maturity Model Certification (CMMC): Draft CMMC Model REV 064 Release & Request for Feedback',* Briefing, Office of the Undersecretary of Defense, Acquisition and Sustainment, U.S. Department of Defense, September 2019. https://www.acq.osd.mil/cmmc/docs/cmmc-overview-brief-30aug19.pdf
4. *Cybersecurity Maturity Model Certification (CMMC): Unclassified Draft Version 0.4,* Office of the Undersecretary of Defense, Acquisition and Sustainment, U.S. Department of Defense, Copyright 2019 Carnegie Mellon University and Johns Hopkins Applied Physics Laboratory, August 30, 2019. https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf
5. *Cybersecurity Maturity Model Certification (CMMC): Unclassified Draft Version 0.6,* Office of the Undersecretary of Defense, Acquisition and Sustainment, U.S. Department of Defense, Copyright 2019 Carnegie Mellon University and Johns Hopkins Applied Physics Laboratory, November 7, 2019. https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf
6. *Cybersecurity Maturity Model Certification (CMMC): Unclassified Draft Version 0.4,* Office of the Undersecretary of Defense, Acquisition and Sustainment, U.S. Department of Defense, Copyright 2019 Carnegie Mellon University and Johns Hopkins Applied Physics Laboratory, December 16, 2019. https://www.acq.osd.mil/cmmc/docs/cmmc-draft-model-30aug19.pdf

Acronyms

ACRONYM	DESCRIPTION
ACI	Additional Control Item
ACSC	Australian Cyber Security Centre
AIA	Aerospace Industries Association
APL	Johns Hopkins University Applied Physics Laboratory
CERT	Computer Emergency Response Team
CERT®	CERT™ / CERT® is a mark owned by Carnegie Mellon University
CERT®-RMM	CERT® Resilience Management Model
CIS	Center for Internet Security
CIS CSC	CIS Critical Security Controls
CMMC	Cybersecurity Maturity Model Certification (Copyright of Carnegie Mellon University and Johns Hopkins University)
CMMI	Capability Maturity Model Integration
CMMI®	CMMI® is a registered mark owned by Carnegie Mellon University
CMU	Carnegie Mellon University
CNSS	Committee on National Security Systems
CNSSI 1253	Committee on National Security Systems Instructions 1253 *"Security Categorization and Control Selection for National Security Systems"*
CSF	NIST Cybersecurity Framework
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIB ISAC	Defense Industrial Base Information Sharing and Analysis Center
DNS	Domain Name Service
DoD	Department of Defense
DoD OIG	Department of Defense Office of the Inspector General
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
ISO	International Organization for Standardization
NAS	National Aerospace Standards
NCX	National Cyber Exchange
NIST	National Institute of Standards and Technology
NSS	National Security System
RCI	Referenced Control Item
RMF	Risk Management Framework
SEI	Software Engineering Institute of Carnegie Mellon University (an FFRDC)
SEI-CERT®	The CERT Division of the SEI
SME	Subject Matter Expert
UK NCSC	United Kingdom National Cyber Security Centre