Preliminary Analysis of CMMC v0.4

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

Abstract

The motivation behind developing the CMMC for defense contractors is discussed. The significant increase in the number of compliance items and complexity imposed by multiple cybersecurity frameworks and standards is quantified and described. The potential threat to small businesses is made clear. A call to action for small and medium business is put forward so that important feedback is provided to DoD so that an appropriate design is achieved and balanced with respect to the competing demands of good security and affordable, achievable implementation of the core competencies of Information Security.

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

Steve Lines
President DIB ISAC Inc.

Jennifer Kurtz
Cyber Program Director
Manufacturer's EDGE

BLUF (Bottom Line Up Front)

The Inspector General report and the report provided by Sera-Brynn indicated that the implementation of NIST SP 800-171 had failed – the implementation, not the security requirements. So, it would be logical to want to fix the problem – the implementation and enforcement. All the discussion to date regarding the CMMC is around developing a new standard. Performing risk analyses and adding controls where needed is a reasonable thing to do. But to do so accurately, the operational objectives and boundaries need to be defined. Major increases in complexity may actually work against successful implementation of good cybersecurity practices, making it more difficult for small businesses to reach maturity levels concomitant with meaningful program participation.

The CMMC offers constructive improvements to the current guidance But the operational objectives at each level must be defined to ensure a fair system and to allow proper control selection.

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.

Preliminary Analysis of CMMC v0.4

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

The Department of Defense has put the development and implementation of the CMMC on a fast track calling for the finalization of the framework early in 2020 and full implementation by the 3rd quarter of 2020. Recognizing this, we decided to extend our discussion on cyber regulation to include a description of the CMMC and begin the discussion of what it means to defense contractors and their DFARS compliance efforts.

As of this date, the government has produced a number of versions of the CMMC with Version 0.4 as the latest. It was released for comments and the comments were due September 25, 2019. A second comment period is coming in November 2019 on Version 0.6, so getting comments together and submitted is still very important. The National Cyber Exchange (NCX) has partnered with the Defense Industrial Base Information Sharing and Analysis Center (DIB ISAC) to collect comments and submit them to DoD. It is the hope of NCX and DIB ISAC to give a strong voice to small and medium sized defense contractors in this process. All contractors are invited to submit their comments at https://nationalcyber.org/CMMC . The DIB ISAC and NCX plan to keep the web site open and active until the CMMC is finalized. So, with enough businesses participating, strong statements will be made possible. Please consider participating.

BACKGROUND: WHY DOD IS DEVELOPING THE CMMC

DoD is revising the DFARS compliance requirements because the self-attestation of fully implementing the security requirements in NIST SP 800-171 did not work. This conclusion was reported in mid-2019 by both the DoD Inspector General (Reference 1) and Sera-Brynn (Reference 2). A summary of key findings is provided in Figure 1 below.

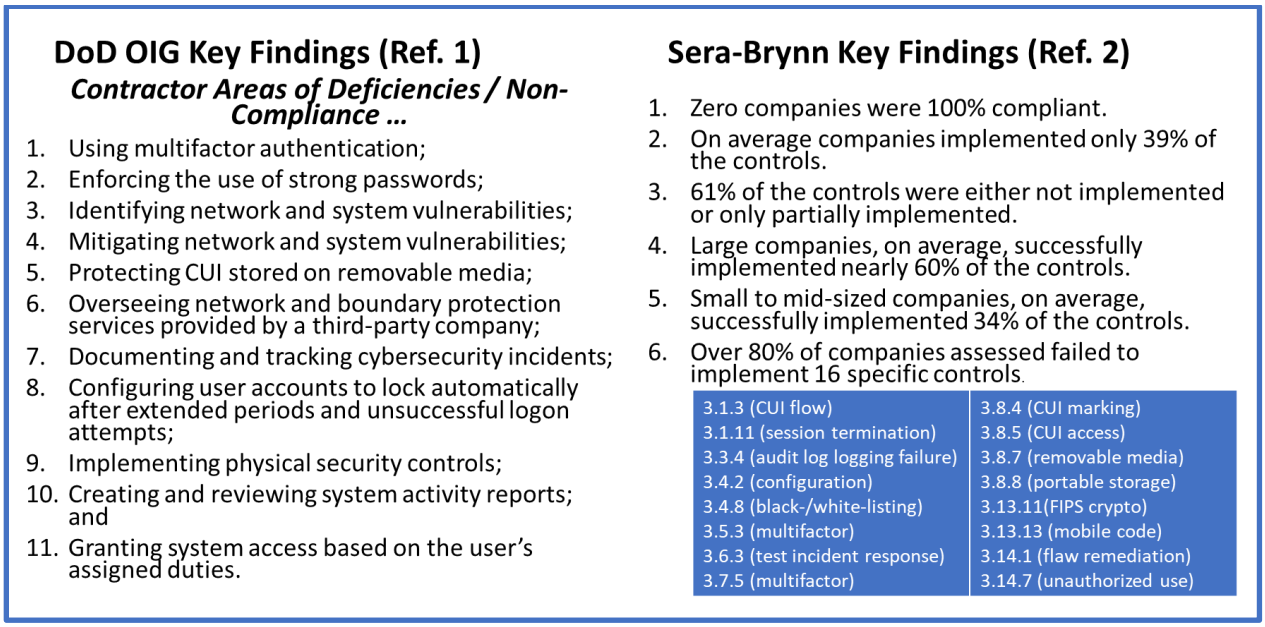

Figure 1 Key Audit Findings

In response to these findings, DoD made the decision to revise the DFARS program for defense contractors. They have determined that:

1. Contractors must be certified by a qualified third party,
2. A five-level maturity model will be incorporated into the new model, and
3. DoD is considering the use of multiple frameworks and standards.

As of Version 0.4, at least eight different frameworks and standards are included in the CMMC.

Failure to successfully implement the security requirements contained within NIST SP 800-171 was cited as the overarching problem with the initial rollout of the DFARS cybersecurity provision and NIST SP 800-171. DoD has stated it will provide third-party auditors to certify contractors at a specific level of maturity. However, it has provided little information on the implementation approach. Most of the discussions have been focused on the definition of the CMMC. Therefore, an analysis of the CMMC is provided below.

WHAT IS THE CMMC?

DoD has engaged Carnegie Mellon University (CMU) and Johns Hopkins University Applied Physics Laboratory LLC (APL) to develop the CMMC. The model incorporates the maturity concepts from the Carnegie Mellon CMMI (Capability Maturity Model Integration) and the CERT®-RMM (Resilience Management Model), where CERT® is a division of the Software Engineering Institute (SEI), a FFRDC (Federally Funded Research and Development Center) at CMU.

The CMMC, which DoD refers to as a "*new standard and model*" is organized into 18 **domains**, each containing a number of **capabilities**, which in turn call for multiple **practices** and **processes** as shown in Figure 2. The model in version 0.4 also includes security controls of various types from a number of different standards as described in Reference 3. The DoD briefings tally the domains, capabilities, practices , and processes but not the other compliance items. These will be included in this analysis.

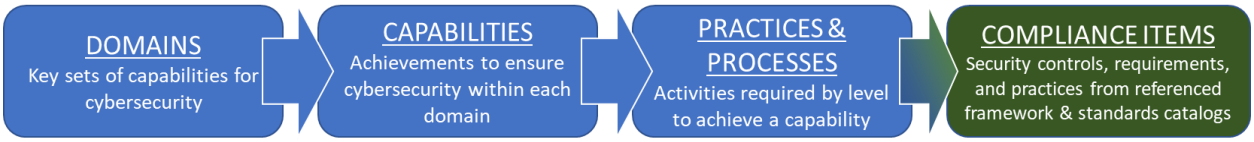

Figure 3 CMMC Hierarchy

Domains contain key sets of capabilities for cybersecurity. Capabilities are the security controls required to ensure cybersecurity. Practices & Processes are activities required to achieve an overall capability defined at each of five levels. As shown in Figure 3, the practices achieve five levels of capabilities and the processes are assessed to determine the five levels of maturity.

The CMMC 18 domains are compared to the 14 security families in NIST SP 800-171 as shown in Figure 4 below.

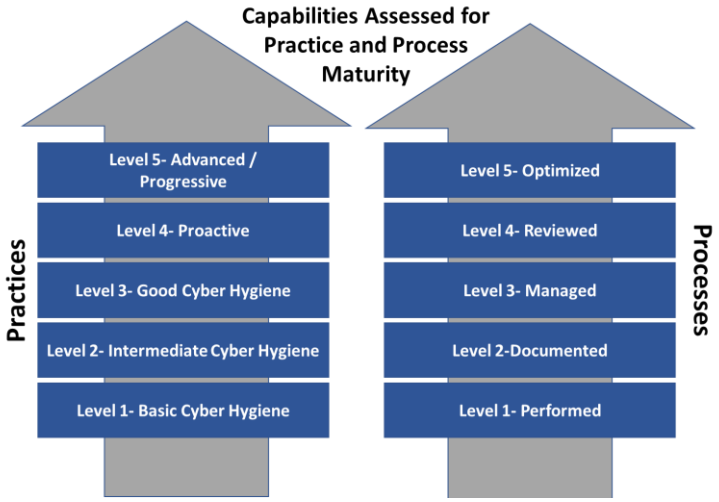

Figure 2 The Five Levels of Maturity in CMMC

	CMMC Domains		NIST 800-171 Families
1	Acces Control (AC)	1	Access Control (AC)
2	Asset Management (AM)		
3	Audit & Accountability (AU)	3	Audit & Accountability (AU)
4	Awareness & Training (AT)	2	Awareness & Training (AT)
5	Configuration Management (CM)	4	Configuration Management (CM)
6	Cybersecurity Governance (CG)		
7	ID & Authorization (IDA)	5	Identification and Authentication (IA)
8	Incident Response (IR)	6	Incident Response (IR)
9	Maintenance (MA)	7	Maintenance (MA)
10	Media Protection (MP)	8	Media Protection (MP)
11	Personnel Security (PS)	9	Personnel Security (PS)
12	Physical Protection (PP)	10	Physical Protection (PP)
13	Recovery (RE)		
14	Risk Management (RM)	11	Risk Assessment (RA)
15	Security Assessment (SAS)	12	Security Assessment (SA)
16	Situational Awareness (SA)		
17	System & Comms Protection (SCP)	13	System and Communications Protection (SCP)
18	System & Info. Integrity (SII)	14	System and Information Integrity (SII)

Figure 4 CMMC Domains Compared to Security Families of NIST SP 800-171

The CMMC, as defined in Reference 4, defines the capabilities within each domain. A sample of the CMMC model is provided in Figure 5. Each domain has a number of capabilities identified in the left column and the practices required at each level are defined, indicating both the capability and level to which the practice belongs. Below the defined CMMC practice, the additional compliance items are cited. Each domain will contain nine processes that define the level of maturity. A sample maturity capability is shown in Figure 6.

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
C1 Establish internal system access requirements	L1-1 System access is limited to authorized users, processes acting on behalf of authorized users, and devices, at least in an ad hoc manner. • NIST SP 800-171 3.1.1	L2-1 The organization has a process to limit system access to authorized users, processes acting on behalf of authorized users, and devices • NIST SP 800-171 3.1.1			
		L2-2 System logon screens display the appropriate system use notification messages. • NIST SP 800-171 3.1.9			
C2 Control internal system access	L1-1 Limit system access to the types of transactions and functions that authorized users are permitted to execute. • NIST SP 800-171 3.1.2	L2-1 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 3.1.4	L3-1 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 3.1.6	L4-1 The organization comprehensively applies least privilege and separation of duties to identities, processes, networks, and interfaces across the enterprise. • DIB	L5-1 Network, host, and software access management is context-aware, adapting the security posture to the most restrictive viable settings based on the physical location, network connection state, time-of-day, and measured properties of the current user and role. • DIB
	L1-2 Limit unsuccessful logon attempts on a single system to 10 or less. • NIST SP 800-171 Partial 3.1.8	L2-2 Only grant privileges necessary for a system user to fulfill their assigned duties. • NIST SP 800-171 3.1.5	L3-2 Role based access is implemented to prevent non-privileged users from executing privileged functions. • NIST SP 800-171 3.1.7	L4-2 The system performs recurring scans and assessments to ensure appropriate user permissions are maintained. • CSF: PR.AC-2, PR-AC-3, PR.AC-4 • CIS: 14.5	L5-2 The organization ensures that all access to systems, services, and networks is indirect, managed via a service mediation layer that provides secure transaction processing, monitoring, and policy enforcement while hiding logical and physical locations and access methods from the accessing user, application, or service. • DIB
		L2-3 All wireless access is authorized prior to allowing such connections. • NIST SP 800-171 3.1.16	L3-3 The execution of privileged functions is recorded in audit logs. • NIST SP 800-171 3.1.7	L4-3 The organization utilizes a wireless intrusion detection system to identify and alert on unidentified wireless access points connected to the network. • CIS 7.1 • CIS 15.3	

Figure 5 Sample CMMC Table

DOMAIN: ACCESS CONTROL (AC)					
MATURITY LEVEL CAPABILITY	PROCESSES				
	Maturity Level 1 (ML1)	Maturity Level 2 (ML2)	Maturity Level 3 (ML3)	Maturity Level 4 (ML4)	Maturity Level 5 (ML5)
Improve Access Control activities		ML2-1 Establish a policy for Access Control.	ML3-1 Review Access Control activities for conformance.	ML4-1 Inform high-level management.	ML5-1 Standardize documentation for Access Control.
		ML2-2 Establish practices to implement Access Control.	ML3-2 Provide resources for Access Control.	ML4-2 Review Access Control activities for effectiveness.	ML5-2 Share Access Control improvements across the organization.
		ML2-3 Establish a plan for Access Control.			

Figure 4 Sample Maturity Processes for Each Domain

WHAT IS THE COMPLEXITY AND DEGREE OF DIFFICULTY OF THE CMMC?

The NIST SP 800-171 was derived from the NIST Risk Management Framework (RMF) and the Federal Information Processing Standards (FIPS) moderate baseline. Although the FIPS utilize full security controls from the NIST SP 800-53 catalog of controls, NIST SP 800-171 contains 110 more basic "requirements," which refer back to NIST SP 800-53 controls for reference.

The CMMC reverses the previous attempt to simplify and minimize the total number of controls or requirements. The current version (v0.4) uses the following list of frameworks and standards (Figure 7), four of which are proprietary (indicated by highlighting). By contrast, the current system uses NIST SP 800-171 alone, but does reference a number of NIST SP 800-53 controls for additional guidance.

CMMC Standards & Frameworks	Current DFARS NIST SP 800-171 Standards & Frameworks
1. NIST SP 800-171 2. NIST SP 800-171B 3. NIST SP 800-53 4. NIST CSF 1.1 (Cybersecurity Framework) 5. ISO 27001:2013 6. AIA NAS 9933 7. CIS CSC 7.1 8. CERT RMM 9. DIB SCC TF WG Top 10 10. Additional DIB Inputs 11. SME (Subject Matter Experts) Input	1. NIST SP 800-171 2. References to the NIST Risk Management Framework (RMF) Controls in NIST SP 800-53

Figure 5 CMMC Frameworks and Standards

Presentations by DoD have indicated that the design objectives of the CMMC are to follow NIST SP 800-171 guidelines to qualify contractors at Level 3; below Level 3 would be the FAR requirements and above would incorporate NIST SP 800-171B. The analysis in Figure 8, however, shows that this is not fully accurate. Most of the NIST SP 800-171 security requirements are used by Level 3 but certifying to Level 3 will require compliance with several controls from NIST SP 800-171B, RMM, ISO 27001, CSF, CIS, and the DIB. In total, 11 sources of controls or practices have been cited in the CMMC, nine of which are stand-alone standards or frameworks. The four highlighted standards and frameworks are proprietary, and DoD has not said that free access would be provided to these standards.

The cumulative number of additional control items requiring compliance is shown in Figure 9. These are additional control items to the practices and processes specified in the CMMC. NIST SP 800-171 security

requirements represent 34% of all additional control items. The cumulative number of these is 278, with Level 3 requiring 187 additional control items.

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
NIST 800-171	23	49	49	2	1
NIST 800-171B	0	0	1	19	7
NIST 800-53	0	0	0	1	0
RMM	13	35	23	9	1
ISO 27001:2013	0	5	2	1	0
CSF	1	1	1	36	1
CIS	1	5	6	22	3
DIB[(1)]	0	0	24	24	27
TOTALS	38	95	106	114	40

Note 1: The DIB 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 DIB citings is shown.

Figure 8 Number of Unique Control Items Cited by CMMC

The items shown in Figure 9 **are not** the practices and processes specified in CMMC. They are the controls, categories, and requirements from other standards and frameworks that are cited by the CMMC. For simplicity, these are referred to in this paper as additional compliance items or ACIs. The number of ACIs required at Level 3 is 187, a 70% increase over the 110 security requirements contained in NIST SP 800-171.

Turning to the practices and processes spelled out in the CMMC, the analysis shows that a large number of these items require compliance as well. The total number of practices specified in the CMMC for each domain is shown in Figure 10. The highlighted cells indicate areas where the author's count varied slightly from the DoD briefing. The largest number of controls are within the domains of Access Control, Incident Response, and Risk Management. The cumulative number of practices needed for Level 3 is 244, and for Level 5 the cumulative number of practices is 386. The 244 practices at Level 3 is more than double the number of security requirements—and this number does not include ACIs.

	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5	TOTAL	% OF TOTAL
NIST 800-171	23	50	94	94	94	94	34%
NIST 800-171B	0	0	1	19	25	25	9%
NIST 800-53	0	0	0	1	1	1	0%
RMM	13	36	47	50	51	51	18%
ISO 27001:2013	0	5	7	8	8	8	3%
CSF	1	2	2	38	39	39	14%
CIS	1	6	12	33	36	36	13%
DIB[(1)]	0	0	24	24	24	24	9%
TOTALS	38	99	187	267	278	278	100%

Note 1: The DIB 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 DIB citings is shown.

Figure 9 Cumulative Unique Control Items in v0.4 CMMC

	CMMC Domains	Capabilities Total	Practices Total	LEVEL 1 Practices	LEVEL 2 Practices	LEVEL 3 Practices	LEVEL 4 Practices	LEVEL 5 Practices	TOTALS Practices Total
1	Acces Control (AC)	5	40	5	9	12	5	9	40
2	Asset Management (AM)	4	16	2	5	4	5	0	16
3	Audit & Accountability (AA)	8	26	2	9	7	7	1	26
4	Awareness & Training (AT)	4	16	0	4	5	7	0	16
5	Configuration Management (CM)	5	21	2	8	4	6	1	21
6	Cybersecurity Governance (CG)	4	21	2	6	4	9	0	21
7	ID & Authorization (IDA)	2	17	2	1	9	2	3	17
8	Incident Response (IR)	9	41	3	15	7	9	7	41
9	Maintenance (MA)	2	9	1	5	2	1	0	9
10	Media Protection (MP)	8	13	1	6	5	0	1	13
11	Personnel Security (PS)	2	5	2	2	0	1	0	5
12	Physical Protection (PP)	5	17	4	10	3	0	0	17
13	Recovery (RE)	2	8	0	3	3	2	0	8
14	Risk Management (RM)	7	36	0	9	6	15	6	36
15	Security Assessment (SAS)	6	16	1	6	2	6	1	16
16	Situational Awareness (SA)	4	17	2	2	3	7	3	17
17	System & Comms Protection (SCP)	3	45	2	10	13	12	8	45
18	System & Info. Integrity (SII)	5	13	4	5	0	2	2	13
	Practices & Controls TOTALS	85	377	35	115	89	96	42	377
	Maturity Processes TOTALS		9	0	3	2	2	2	9
	Practices, Processes & Controls ACCUMULATIVE TOTALS	85	386	35	153	244	342	386	386

Figure 10 CMMC Capabilities and Practices by Domain and Level

Level 3 is identified as a key target for contractor qualification. It is generally believed that this is the minimum qualification for contractors to perform significant contract work involving CUI. The AIA NAS 9933 (Aerospace Industries Association / National Aerospace Standards) standard specifically states that Level 3 is the minimum qualifying level. The recent briefings and descriptions provided by DoD offer no information as to what work can be performed at each of the five levels. In fact, no information is provided on how to use the "model" nor how it is going to be implemented. So, this analysis assumes that Level 3 is a key or critical level for contractors, just as it is in the AIA NAS 9933 document.

Staying with the Level 3 evaluation, the 244 practices show a significant increase in number (122%) and, with eight different frameworks and standards, a great increase in complexity or degree of difficulty in achieving compliance. This increase in numbers and complexity is doubled again when the ACIs are added to the number of practices. Figure 11 below shows the same table of practices by domain and includes the number of compliance items by domain. The figure shows that a total of 521 practices, processes, and ACIs are required at Level 3. This is a 374 % increase in the number of implementation requirements. The DoD briefing stated that DoD had not yet down-selected (without defining what that means). This analysis suggests that down-selecting needs to be major and significant.

In addition, no guidance has been given on how to use the model. Therefore, the down-select process may result in guidance that is not actually required to achieve compliance with all practices and control items. This begs the question: Why would controls and practices be articulated if not for compliance? More to come here.

Figure 11 Practices, Processes and Compliance Items by Domains of CMMC

	CMMC Domains	Capabilities Total	LEVEL 1		LEVEL 2		LEVEL 3		LEVEL 4		LEVEL 5		TOTALS	
			Practices	Controls	Practices	Controls	Practices	Controls	Practices	Controls	Practices	Controls	Practices Total	Controls Total
1	Acces Control (AC)	5	5	5	9	9	12	12	5	9	9	9	40	44
2	Asset Management (AM)	4	2	3	5	7	4	4	5	4	0	0	16	18
3	Audit & Accountability (AA)	8	2	3	9	11	7	8	7	7	1	1	26	30
4	Awareness & Training (AT)	4	0	0	4	6	5	7	7	16	0	0	16	29
5	Configuration Management (CM)	5	2	3	8	12	4	4	6	7	1	1	21	27
6	Cybersecurity Governance (CG)	4	2	2	6	6	4	4	9	13	0	0	21	25
7	ID & Authorization (IDA)	2	2	2	1	1	9	9	2	2	3	2	17	16
8	Incident Response (IR)	9	3	3	15	18	7	7	9	9	7	2	41	39
9	Maintenance (MA)	2	1	2	5	6	2	2	1	2	0	0	9	12
10	Media Protection (MP)	8	1	1	6	11	5	8	0	0	1	1	13	21
11	Personnel Security (PS)	2	2	2	2	4	0	0	1	3	0	0	5	9
12	Physical Protection (PP)	5	4	5	10	12	3	3	0	0	0	0	17	20
13	Recovery (RE)	2	0	0	3	5	3	4	2	2	0	0	8	11
14	Risk Management (RM)	7	0	0	9	13	6	5	15	18	6	7	36	43
15	Security Assessment (SAS)	6	1	1	6	6	2	2	6	10	1	1	16	20
16	Situational Awareness (SA)	4	2	2	2	2	3	3	7	15	3	3	17	25
17	System & Comms Protection (SCP)	3	2	2	10	10	13	11	12	13	8	8	45	44
18	System & Info. Integrity (SII)	5	4	4	5	5	0	0	2	3	2	3	13	15
	Practices & Controls TOTALS	85	35	40	115	144	89	93	96	133	42	38	377	448
	Maturity Processes TOTALS		0		3		2		2		2		9	
	Practices, Processes & Controls ACCUMULATIVE TOTALS	85	35	75	190	337	426	521	617	752	794	834	377	834

Figure 12 shows the five levels of the CMMC compared to other significant standards, baselines, and overlays. The five CMMC levels are shown in red. This figure shows that CMMC Level 3 has more controls and compliance items than the highest risk, the critical national security system as defined by the CNSSI 1253 (Committee for National Security Systems Instructions). It shows that it is about equal to the FIPS enhanced baseline.

It is recognized that treating all controls, requirements, and practices the same is not totally accurate. But they all require compliance and it is an enormous number of items to track, achieve compliance with, and provide evidence of compliance to an outside auditor.

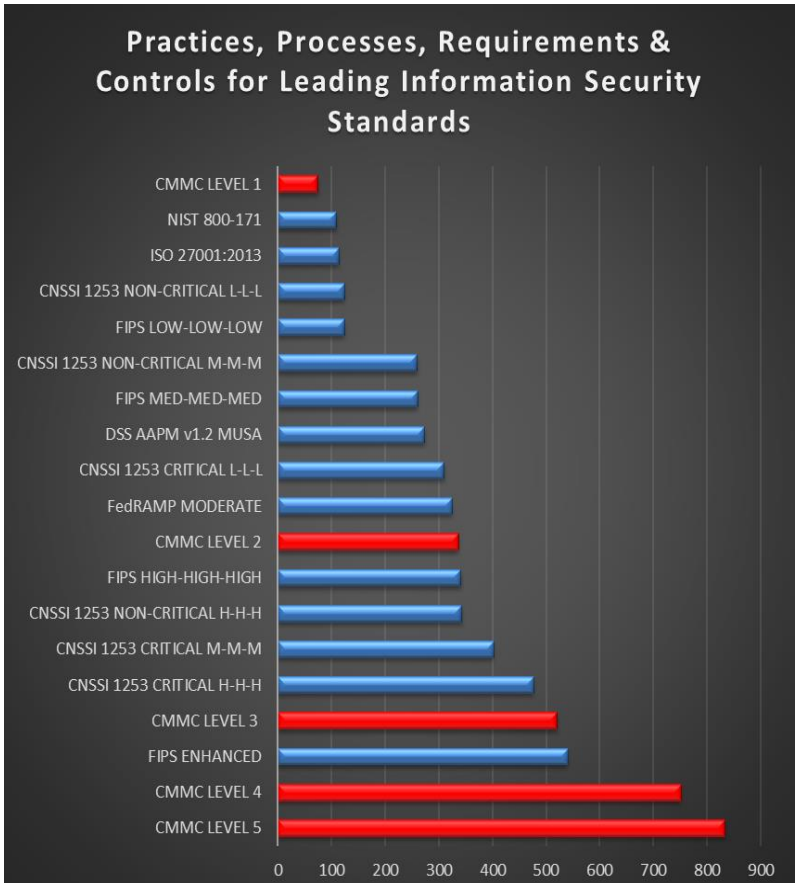

Figure 12 CMMC Levels Compared to Other Security Baselines

WHY ARE SO MANY FRAMEWORKS AND STANDARDS REQUIRED?

The basic process followed in designing an information security system includes risk analysis, selection of a risk framework appropriate for the application, and building the defense of the system with the selection of controls from a control catalog. The two major risk frameworks are the NIST RMF (Risk Management Framework) combined with the NIST SP 800-53 catalog, and the ISO 27001, for which ISO 27002 is the controls catalog.

NIST SP 800-171 was derived from the RMF, specifically the FIPS (Federal Information Processing Standards) moderate baseline. Items pertaining to the government were discarded. Controls not pertaining to confidentiality were likewise discarded. Finally, a number of items were defined as non-federal organization (NFO) capabilities that organizations were reasonably expected to have in place already. Thus, NIST SP 800-171 was intended to be a good introductory standard for information security and it was recognized that it was optimized for confidentiality at the expense of data integrity and availability.

Performing risk analysis and adding controls to address identified risks is not only a reasonable thing to do but the right thing to do. Unfortunately, the risk analysis that led to the selection of the CMMC controls was not shared. It is a reasonable to assume, however, that any necessary controls can be found in the NIST standards including the RMF, CSF, NIST SP 800-171, and NIST SP 800-171B.

To be clear, each guideline, framework, and standard is excellent in its own right. The CERT-RMM isdesigned for resilience, CIS has very useful benchmarking, ISO is an outstanding standard and framework, and the NIST Special Publications are fast becoming the top cybersecurity guidance in the U.S. and beyond. The issue is dealing with all of them at the same time. It is overwhelming and substantially increases the complexity, degree of difficulty—and cost—of compliance.

WHY ARE SO MANY CONTROLS, PRACTICES, AND PROCESSES REQUIRED?

DoD has stated in its presentations that a down-selection process is to be performed. This down-selection needs to be significant. The Defense Counterintelligence and Security Agency (DCSA) has defined a baseline for a multiple user stand alone (MUSA) system with 274 controls. CMMC Level 3 does not need more than that! NIST SP 800-171 in its current form ensures that security core competencies are implemented—if NIST SP 800-171 is properly implemented and verified.

THE MISSING COMPONENT

The unknown unknown is the definition of the work to be performed at each level of maturity. Is the assumption that the CMMC will, like the AIA NAS 9933, require Level 3 for important work? The guidance provided in the DoD briefings indicate 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. Without understanding the operational aspects of the CMMC, it is difficult to comment intelligently. DoD needs to clarify this information. Without a good definition and common understanding, the CMMC could be used as a procurement screen in a very arbitrary manner.

SUMMARY

The Inspector General report and the report provided by Sera-Brynn indicated that widespread implementation of NIST SP 800-171 security requirements had failed—the implementation, not its substance. The NIST guidelines for cybersecurity are arguably the best in the world. Successful implementation of NIST SP 800-171 security requirements by the majority of defense contractors would have made a meaningful contribution to the collective cybersecurity posture.

It would be logical then to want to fix the problem—the unsuccessful implementation and enforcement. All the discussion to date regarding the CMMC concerns developing a new standard. Performing risk analyses and adding controls where needed is a reasonable thing to do. But to do so accurately, the operational objectives and boundaries need definition.

Furthermore, careful consideration of the quantity of security requirements, their complexity, and degree of difficulty also need to take place. The number of practices, processes, and AICs may only be a proxy for calculating the added complexity of the CMMC model, but they show a five-fold, a nearly 400%, increase in the number of compliance items at Level 3.

The CMMC may offer constructive improvements to NIST SP 800-171. The operational objectives at each level must be defined, however, to ensure a fair system and to allow proper control selection.

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. U.S. Department of Defense, Inspector General, *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems (July23, 2019).* *https://www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-controlled-unclassified-information-on-contractor-ow/*
2. Sera-Brynn, *Reality Check: Defense industry's implementation of NIST SP SP 800-171, Keen insights from certified cybersecurity assessors (May 2019).* https://sera-brynn.com/an-analyst-perspective-sera-brynns-report-on-nist-SP 800-171-is-compliance-achievable/
3. *'Cybersecurity Maturity Model Certification (CMMC): Draft CMMC Model REV 0.4 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

Acronyms

ACRONYM	DESCRIPTION
ACI	Additional Control Item
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
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DIB ISAC	Defense Industrial Base Information Sharing and Analysis Center
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
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