Cybersecurity Maturity Model Certification: A Planning Guide

On January 31, 2020, the U.S. Department of Defense (DoD) released Version 1.0 of its standard for the Cybersecurity Maturity Model Certification (CMMC). The arrival of this cybersecurity framework has government contractors scrambling to reach compliance to ensure continued business. In this paper, Rimstorm, a Managed Security Service Provider (MSSP) based out of Northern Virginia, provides a short explanation of the CMMC, the timeline for its institution, and its implications for continued business with the DoD.

What is CMMC?

The DoD's Cybersecurity Maturity Model Certification (CMMC) is the new standard for DoD contracts that will take the place of NIST 800-171 compliance. CMMC builds upon the existing cybersecurity standards and practices under NIST 800-171, but unlike other maturity models, it adds five levels of process maturity and cybersecurity practices required by a contractor. CMMC addresses the issues faced with previous cybersecurity programs by the creation of certification levels and third-party certification. The DoD's mission statement on the creation of CMMC emphasizes the utmost importance of cybersecurity within defense contractors for continued business with the DoD.

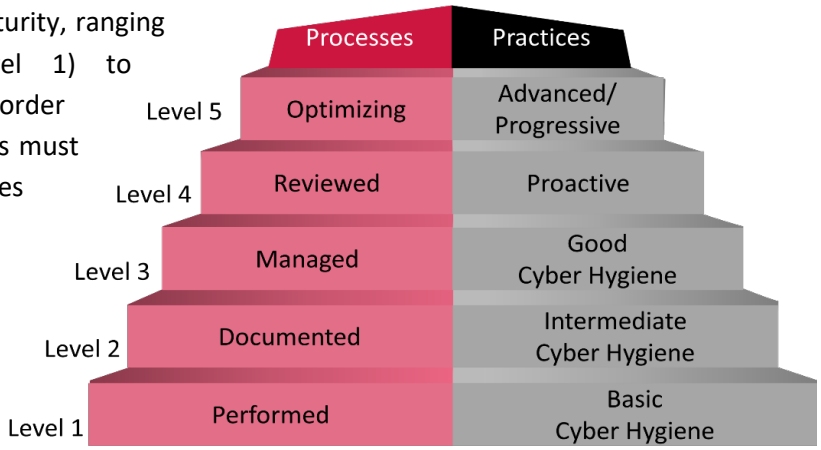
- If your company currently meets standards under NIST 800-171, you may be further along in your CMMC compliance than you think.
- If you have never met NIST 800-171 standards, you can still become certified under CMMC. This is the time to begin your certification work if you have not done so.
- If you are with a small company that does not yet do work with the DoD but are planning to, this certification pertains to you as well. It is best to get certified when you are still small, allowing your policies and procedures to grow with you, keeping them aligned with CMMC requirements along the way.

Why CMMC?

The DoD's significant concern about cybersecurity in the defense contracting space is not without merit and has made protecting the DoD supply chain from cyber attacks a top priority. Previously, DoD contractors could reach compliance through *self-assessment* of NIST 800-171 standards. Because of the lack of third-party validation, the DoD was concerned over the security measures in place to protect critical information. In addition, the *limited adoption* of NIST 800-171 led the DoD to seek other ways of ensuring that their contractors are implementing and maintaining the appropriate levels of cybersecurity required for their businesses. The release of the CMMC framework calls for the integration of NIST 800-171 and additional security standards with actual levels of enforcement from the DoD.

The five-level maturity spectrum for cybersecurity[1]

The CMMC model has five levels of maturity, ranging from "Basic Cyber Hygiene" (Level 1) to "Advanced/Progressive" (Level 5). In order meet a certain CMMC level, contractors must meet the set processes and practices within each level. The current CMMC levels and their processes and practices are shown in the model to the right.



Note that the model here consists both of maturity processes *and* cybersecurity best practices. That is to say, *both the left side and the right side of the figure must be implemented and institutionalized*, and achieving one side does not imply that a company has achieved the other. At a minimum, any company handling Controlled Unclassified Information (CUI) will be required to meet the requirements of Level 3, Managed Processes/Good Cyber Hygeine Practices as well as all of the levels below it.

As shown in the following table, Level 3 represents all 110 of the practices and controls specified in the NIST 800-171 standard, along with 20 additional practices.

CMMC Model Version 1.0 Practices per Level[2]					
CMMC	**Total**	**48 CFR 52.204.21**	**NIST SP 800-171r1**	**Draft NIST 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	16	-	-	4	11
Total	171	15	110	15	46

* Note: 15 safeguarding requirements from 48 CFR 52.204-21 correspond to 17 security requirements in NIST SP 800-171.

These standards and practices encompass 43 capabilities across 17 capability domains. These domains, shown below, originate from the security-related areas of the Federal Information Processing Standards (FIPS) Publication 200 and their related families from NIST 800-171 with the inclusion of three additional domains—Asset Management (AM), Recovery (RE), and Situational Awareness (SA).

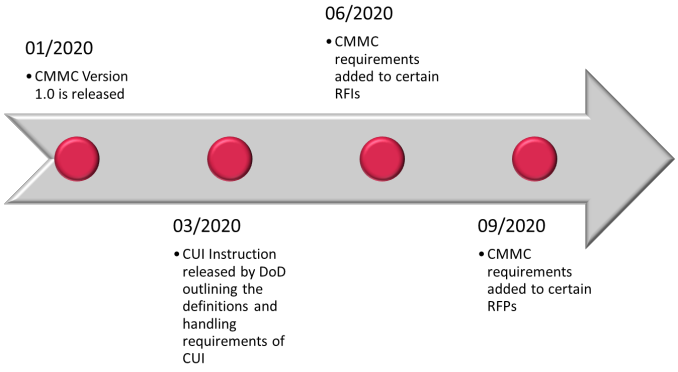
[1] Cybersecurity Maturity Model Certification Version 1.0, January 30, 2020, page 4.
[2] Cybersecurity Maturity Model Certification Version 1.0, January 30, 2020, page 11.

Access Control (AC)	Asset Management (AM)	Audit and Accountability (AA)	Awareness and Training (AT)	Configuration Management (CM)
Identification and Authentication (IDA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)
Physical Protection (PP)	Recovery (RE)	Risk Management (RM)	Security Assessment (SAS)	Situational Awareness (SA)
System and Communications Protections (SCP)		**CMMC Model Domains[3]**		System and Information Integrity (SII)

Because of these additional controls, even a company that is currently fully compliant with NIST 800-171 still has work to do to comply with all 17 CMMC model domains.

What is the timeline for CMMC compliance?[4]

The arrival and more importantly the timeline of CMMC has many contractors rushing to meet the new requirements. DoD contractors should be aware of the following CMMC timeline:



- January 2020: CMMC Version 1.0 is released.
- March 2020: CUI Instruction released by DoD, outlining the definitions and handling requirements of CUI
- June 2020: CMMC requirements will be added in select RFIs
- September 2020: CMMC requirements will be added in select RFPs

[3] Cybersecurity Maturity Model Certification Version 1.0, January 30, 2020, page 7.
[4] DHG Supply Chain Security and CMMC, March 2020, 13-14.

What can your organization do to comply?

Because of the complexity of information to be audited, it is recommended that DoD contractors seeking to become certified enlist the help of a Managed Security Service Provider (MSSP) specializing in CMMC compliance. An experienced MSSP, such as Rimstorm, will provide your organization the ability to meet requirements and pass a CMMC third-party audit. The DoD has stated that contractors will be unable to bid on select contracts if they do not obtain a CMMC certification before the end of 2020.

Rimstorm can identify and fill gaps in these security requirements in a surprisingly cost-effective and painless manner. Visit our web site at www.rimstorm.com/federal-contractors for more information, and contact us for a free evaluation and price quote today.

Rimstorm was founded in 2017 by our CEO, Ben Gerenstein, and our COO, Erik Briceño. Mr. Gerenstein has grown, cultivated, and sold a number of successful IT companies, including, most recently, an MSP located in the DC metro region. He has received numerous awards over the years, including multiple wins of the Fantastic 50 Award presented by the Virginia Chamber of Commerce to the fastest growing companies in the state. Ben's passion for technology began while pursuing his Bachelor's degree in Computer Science at Colgate University. Throughout his career, Ben has had extensive experience as a senior network engineer and security analyst. He was Director of Network Systems at Dow Jones, and his technical experience includes heading a cybersecurity audit team for the US Naval institute. In addition, Ben has an MBA and is also a Certified Information Systems Security Professional (CISSP). As COO, Erik Briceño oversees the daily operations as well as provides support in the creation and implementation of strategic visions for Rimstorm, in collaboration with the CEO, to achieve sustainable long-term growth. Erik is also the owner of V2 Systems, Inc., one of Northern Virginia's leading Information Technology Managed Service Providers. He is an inspiring leader for its employees and instrumental business partner for its customers.