CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

DRAFT CMMC MODEL REV 0.4 RELEASE & REQUEST FOR FEEDBACK

September 2019

Agenda

- CMMC Overview
- Model Framework
- Model Details
  - Summary of Changes
  - Counts by Level and Domain
  - Examples of Practices by Level
- Feedback Request

CMMC Overview

Introduction

- CMMC Vision
  - Be a **unified cybersecurity standard** for DOD acquisitions to reduce exfiltration of Controlled Unclassified Information (CUI) from the Defense Industrial Base (DIB)

- CMMC Schedule
  - CMMC Rev 1.0 will be released in January 2020
  - Will be included in RFIs starting in June 2020
  - Will be included in RFPs starting in Fall 2020

- Multiple Opportunities for Stakeholder Feedback
  - Listening Tour: Visit the website at www.acq.osd.mil/cmmc/
  - Public comment of draft CMMC Rev 0.4 in September 2019
  - Public comment of draft CMMC Rev 0.6 in November 2019

What is CMMC?

- CMMC is the **Cybersecurity Maturity Model Certification**
  - Combines various cybersecurity standards and “best practices”
  - Maps these practices and processes across several maturity levels that range from basic cyber hygiene to advanced
  - For a given CMMC level, the associated practices and processes, when implemented, will reduce risk against a specific set of cyber threats.

- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.

- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels

- The intent is for certified independent 3rd party organizations to conduct audits and inform risk

Request for Feedback of Draft CMMC Model Rev 0.4

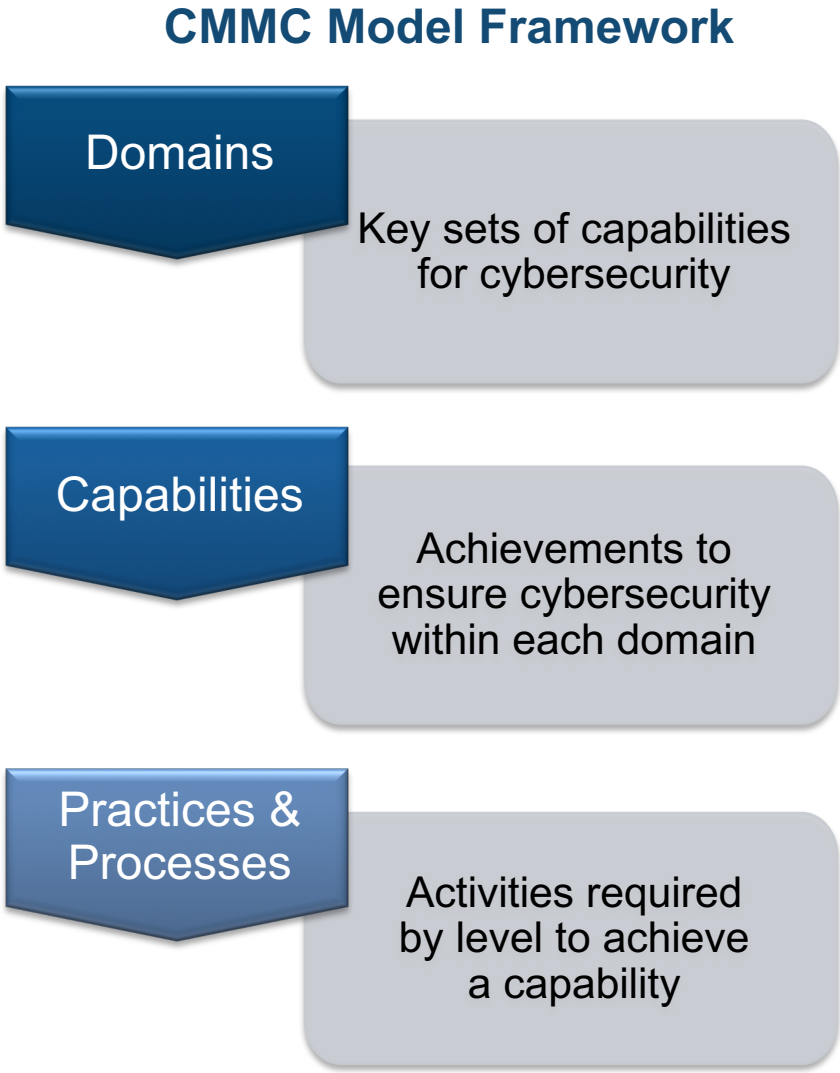
- As you review this midpoint release of the model, please consider:
  - The final version of this model will be released in January 2020
  - The model is still being refined and a reduction in size is anticipated
    - Down selecting, prioritizing, and consolidating capabilities is still to occur
  - Practices within the model have not been cross-referenced across domains or to all references
    - E.g., in the System Integrity domain capability 3 on Malicious Content (SII-C3), there are currently only Level 1 practices focused on antivirus, when there are related higher-level practices that could be added or cross-mapped from other domains in future releases
  - A methodology to handle maturity level trade-offs is planned
  - Detailed assessment guidance is still under development

- Help us by answering these questions:
  1. What do you recommend removing or de-prioritizing to simplify the model and why?
  2. Which elements provide high value to your organization?
  3. Which practices would you move or cross-reference between levels or domains?
  4. In preparation for the pending easy-to-use assessment guidance, what recommendations might you have to clarify practices and processes?

CMMC Model Framework

CMMC Model Framework

- CMMC model framework consists of 18 domains, based on cybersecurity “best practices”
- Domains are comprised of capabilities
- Capabilities are comprised of practices and processes, which are mapped to CMMC Level 1 through Level 5
  - Practices are activities performed at each level for the domain
  - Processes detail maturity of institutionalization for the practices



CMMC Model Level Descriptions

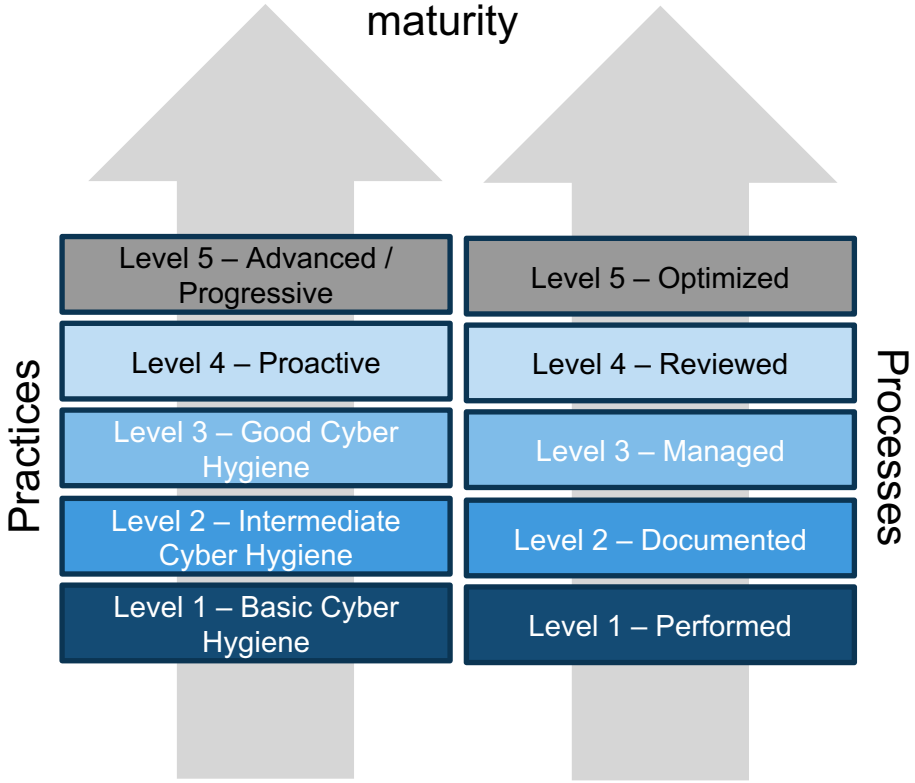
	Description of Practices	Description of Processes
Level 1	• Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions	• Practices are performed, at least in an ad-hoc matter
Level 2	• Inclusive of universally accepted cyber security best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions	• Practices are documented
Level 3	• Coverage of all NIST SP 800-171 rev 1 controls • Additional practices beyond the scope of CUI protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets	• Processes are maintained and followed
Level 4	• Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets	• Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5	• Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most-advanced threat actors • Defensive responses performed at machine speed • Machine performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets	• Continuous improvement across the enterprise

CMMC Model Structure

18 Domains (Rev 0.4)

Access Control	Identification and Authentication	Recovery
Asset Management	Incident Response	Risk Assessment
Awareness and Training	Maintenance	Security Assessment
Audit and Accountability	Media Protection	Situational Awareness
Configuration Management	Personnel Security	System and Communications Protection
Cybersecurity Governance	Physical Protection	System and Information Integrity

Capabilities assessed for Practice and Process maturity



The Importance of Process Maturity

- A subset of industry feedback has highlighted the challenges of being 100% compliant with some practices
  - For example, maintaining a 100% asset inventory over 200k+ machines
- Assessment of process institutionalization helps to mitigate this concern
- Process institutionalization (that is, policies, plans, processes, and procedures to manage the environment where CUI resides) provides assurances that practices are being implemented effectively

A comprehensive assessment of process maturity within the model can **offset the need for 100% compliance** for some practices

CMMC Model Rev 0.4 Details

Model Rev 0.4 Synopsis - Practices

	Description of Level Practices	CMMC Rev 0.3 Practices	New CMMC Rev 0.4 Material	CMMC Rev 0.4 Practices	Rev 0.4 New Content Sources
CMMC Level 1	Basic Cyber Hygiene	17	**+18 practices**	35	• DIB SCC TF WG Top 10 • NIST Cybersecurity Framework 1.1 • ISO 27001:2013 • AIA NAS 9933 • CIS Critical Security Controls 7.1 • CERT Resilience Management Model® • Additional DIB Inputs • Subject Matter Experts
CMMC Level 2	Intermediate Cyber Hygiene	46	**+69 practices**	115	
CMMC Level 3	Good Cyber Hygiene	63	**+28 practices**	91	
CMMC Level 4	Proactive	10	**+85 practices**	95	
CMMC Level 5	Advanced / Progressive	4	**+30 practices**	34	

CMMC Model Rev 0.4 Levels by the Numbers

	Access Control	Asset Management	Audit and Accountability	Awareness and Training	Configuration Management	Cybersecurity Governance	Identity and Authorization	Incident Response	Maintenance	Media Protection	Personnel Security	Physical Protection	Recovery	Risk Management	Security Assessment	Situational Awareness	System & Comms Protection	Systems and Info Integrity
Capabilities	5	4	8	4	5	4	2	9	2	8	2	5	2	7	6	4	3	5
Practices	30	19	27	16	21	21	17	41	9	13	5	17	8	36	15	17	45	13
Level 1	5	2	2	0	2	2	2	3	1	1	2	4	0	0	1	2	2	4
Level 2	9	5	9	4	8	6	1	15	5	6	2	10	3	9	6	2	10	5
Level 3	11	7	7	5	4	4	9	7	2	5	0	3	3	6	2	3	13	0
Level 4	5	5	7	7	6	9	2	9	1	0	1	0	2	15	5	7	12	2
Level 5	0	0	2	0	1	0	3	7	0	1	0	0	0	6	1	3	8	2

Each domain also includes nine standard processes

Down-selection, prioritization, and consolidation is still to occur

Model Rev 0.4 – Examples of Level 1-3 Practices

- Examples of Level 1 Practices
  - FAR requirements
  - Anti-virus
  - Ad hoc incident response*
  - Ad hoc cybersecurity governance*
- Examples of Level 2 Practices
  - Risk management
  - Awareness and training
  - Back-ups & security continuity*
- Examples of Level 3 Practices
  - All NIST SP 800-171 Rev 1 requirements are met
    - Multi-factor authentication
  - Information Security Continuity Plan*
  - Communicate threat information to key stakeholders*

* Example capability not covered by NIST SP 800-171 Rev 1

Model Rev 0.4 – Examples of Level 4-5 Practices

- Examples of Level 4 Practices
  - Consideration of supply chain risk
  - Threat hunting
  - Out-of-band administration
  - Use of Data Loss Prevention (DLP) technologies
  - Detonation chambers
  - Inclusion of mobile devices
  - Network segmentation
- Examples of Level 5 Practices
  - Deployment of organizational custom protections
  - Cyber maneuver operations
  - Hardware root of trust for boot
  - Real-time asset tracking
  - 24x7 SOC operation
  - Context aware access control and step-up authentication
  - Device authentication
  - Autonomous initial response actions

CMMC Levels 4 & 5 are targeted toward a small subset of the DIB sector that supports DOD critical programs and technologies

Feedback Request

Request for Feedback of Draft CMMC Model Rev 0.4

- As you review this midpoint release of the model, please consider:
  - The final version of this model will be released in January 2020
  - The model is still being refined and a reduction in size is anticipated
    - Down selecting, prioritizing, and consolidating capabilities is still to occur
  - Practices within the model have not been cross-referenced across domains or to all references
    - E.g., in the System Integrity domain capability 3 on Malicious Content (SII-C3), there are currently only Level 1 practices focused on antivirus, when there are related higher-level practices that could be added or cross-mapped from other domains in future releases
  - A methodology to handle maturity level trade-offs is planned
  - Detailed assessment guidance is still under development
- Help us by answering these questions:
  1. What do you recommend removing or de-prioritizing to simplify the model and why?
  2. Which elements provide high value to your organization?
  3. Which practices would you move or cross-reference between levels or domains?
  4. In preparation for the pending easy-to-use assessment guidance, what recommendations might you have to clarify practices and processes?

We look forward to your feedback!

Copyright & Distribution Information

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory, LLC, a University Affiliated Research Center.

DM19-0824