CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

Version 1.0 | January 30, 2020

NOTICES

Copyright 2020 Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY AND THE JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY LLC MAKE NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL NOR ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] Approved for public release.

DM19-0824

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. Introduction

The theft of intellectual property and sensitive information from all industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 [1]. The Center for Strategic and International Studies estimates that the total global cost of cybercrime was as high as $600 billion in 2017 [2].

Malicious cyber actors have targeted, and continue to target the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD). The DIB sector consists of over 300,000 companies that support the warfighter and contribute towards the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation as well as significantly increase risk to national security.

As part of multiple lines of effort focused on the security and resiliency of the DIB sector, the DoD is working with industry to enhance the protection of the following types of unclassified information within the supply chain:

- *Federal Contract Information (FCI*): FCI is information provided by or generated for the Government under contract not intended for public release [3].
- *Controlled Unclassified Information (CUI):* CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended [4].

Towards this end, the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) has developed the Cybersecurity Maturity Model Certification (CMMC) framework in concert with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the DIB sector.

This document focuses on the CMMC model which measures cybersecurity maturity with five levels and aligns a set of processes and practices with the type and sensitivity of information to be protected and the associated range of threats. The model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community.

The model encompasses the *basic safeguarding requirements* for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the *security requirements* for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 [3, 4, 5].

The CMMC framework adds a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the DoD that a DIB contractor can adequately protect CUI at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain.

When implementing CMMC, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information to be protected is handled and stored.

1.1 Document Organization

This document is organized as follows. Section 2 presents the CMMC model and each of its elements in detail. Appendix A provides the model as a matrix. Appendix B includes the discussion and clarifications associated with each process and practice in the model. Appendix C is the glossary. Appendix D lists the abbreviations and acronyms. Appendix E maps the CMMC model to other sources. Finally, Appendix F provides the references contained in the document.

2. CMMC Model

2.1 Background on Maturity Models

In general, a *maturity model* is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline. The content of such a model typically exemplifies best practices and may incorporate standards or other codes of practice of that discipline. A maturity model thus provides a benchmark against which an organization can evaluate the current level of capability of its processes, practices, and methods and set goals and priorities for improvement. To measure progression, maturity models typically have *levels* along a scale [9,10].

2.2 Overview

The Cybersecurity Maturity Model Certification (CMMC) framework consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the Defense Industrial Base (DIB) and Department of Defense (DoD) stakeholders. The model framework (Figure 1) organizes these *processes* and *practices* into a set of *domains* and maps them across five *levels*. In order to provide additional structure, the framework also aligns the practices to a set of *capabilities* within each domain. The ensuing subsections provide additional information regarding each element of the model.

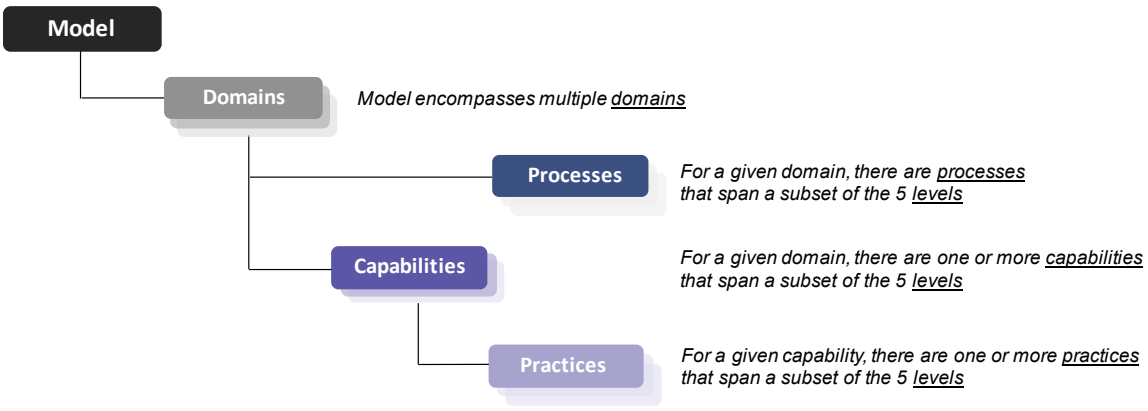

Figure 1. CMMC Model Framework (Simplified Hierarchical View)

2.3 CMMC Levels

2.3.1 Descriptions

The CMMC model measures cybersecurity maturity with five levels. Each of these levels, in turn, consists of a set of processes and practices which are characterized in Figure 2. The

processes range from 'Performed' at Level 1 to 'Optimizing' at Level 5 and the practices range from 'Basic Cyber Hygiene' at Level 1 to 'Advanced/Progressive' at Level 5.

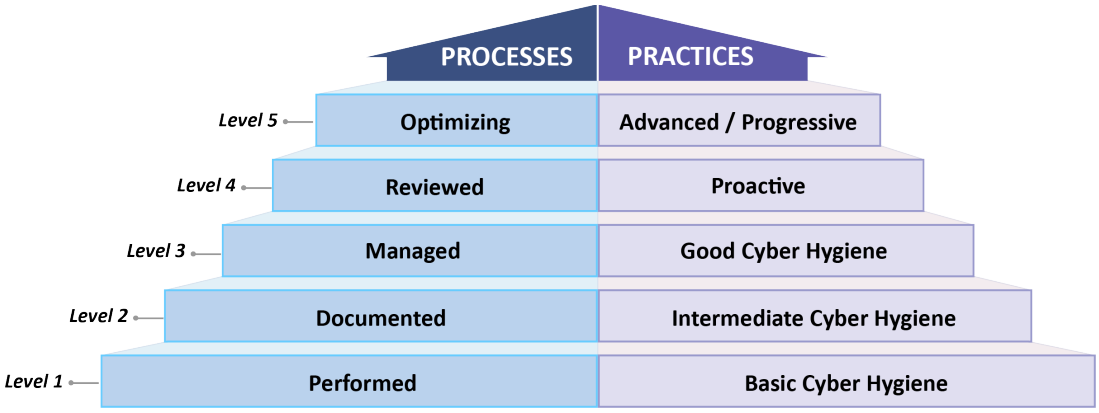

Figure 2. CMMC Levels and Descriptions

The CMMC levels and the associated sets of processes and practices across domains are cumulative. More specifically, in order for an organization to achieve a specific CMMC level it must also demonstrate achievement of the preceding lower levels.

Furthermore, an organization must demonstrate both the requisite institutionalization of processes (i.e., the left side in Figure 2) and the implementation of practices (i.e., the right side in Figure 2) for a specific CMMC level and the preceding lower levels in order to achieve that level. For the case where an organization demonstrates different achievements with respect to process institutionalization and practice implementation, the organization will be certified at the lower of the two levels.

2.3.2 Focus

In addition to the previous CMMC level descriptions, the specification and mapping of processes and practices to a particular level take into account multiple considerations including regulations, type and sensitivity of information, threats, costs, implementation complexity, diversity within the DIB sector, assessment implications, and other factors. The CMMC model, in effect, provides a means of improving the alignment of maturity processes and cybersecurity practices with the type and sensitivity of information to be protected and the range of threats. As a result, the CMMC levels can also be characterized by this alignment or more simply, their focus, as follows:

- Level 1: Safeguard Federal Contract Information (FCI)
- Level 2: Serve as transition step in cybersecurity maturity progression to protect CUI
- Level 3: Protect Controlled Unclassified Information (CUI)
- Levels 4-5: Protect CUI and reduce risk of Advanced Persistent Threats (APTs)

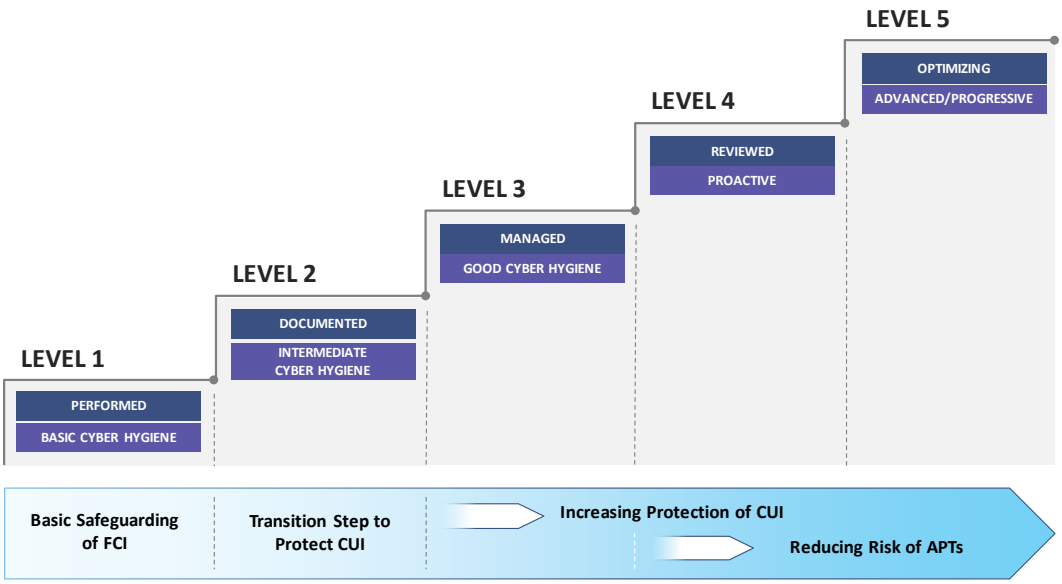

Figure 3. CMMC Levels and Associated Focus

The achievement of higher CMMC levels enhances the ability of an organization to protect CUI and, for Levels 4-5, reduces the risk of APTs (Figure 3). An APT is an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception) [6,11].

2.3.3 CMMC Level 1

- Processes: Performed

  Level 1 requires that an organization performs the specified practices. Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation, process maturity is not assessed for Level 1.

- Practices: Basic Cyber Hygiene

  Level 1 focuses on the protection of FCI and consists only of practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21 ("Basic Safeguarding of Covered Contractor Information Systems") [3].

2.3.4 CMMC Level 2

- Processes: Documented

  Level 2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented.

- Practices: Intermediate Cyber Hygiene
  Level 2 serves as a progression from Level 1 to Level 3 and consists of a subset of the security requirements specified in NIST SP 800-171 [4] as well as practices from other standards and references. Because this level represents a transitional stage, a subset of the practices reference the protection of CUI.

2.3.5 CMMC Level 3

- Processes: Managed
  Level 3 requires that an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders.

- Practices: Good Cyber Hygiene
  Level 3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800-171 [4] as well as additional practices from other standards and references to mitigate threats.

  It is noted that DFARS clause 252.204-7012 ("Safeguarding of Covered Defense Information and Cyber Incident Reporting") [5] specifies additional requirements beyond the NIST SP 800-171 security requirements such as incident reporting.

2.3.6 CMMC Level 4

- Processes: Reviewed
  Level 4 requires that an organization review and measure practices for effectiveness. In addition to measuring practices for effectiveness, organizations at this level are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis.

- Practices: Proactive
  Level 4 focuses on the protection of CUI from APTs and encompasses a subset of the enhanced security requirements from Draft NIST SP 800-171B [6] as well as other cybersecurity best practices. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques, and procedures (TTPs) used by APTs.

2.3.7 CMMC Level 5

- **Processes: Optimizing**
  Level 5 requires an organization to standardize and optimize process implementation across the organization.

- **Practices: Advanced/Proactive**
  Level 5 focuses on the protection of CUI from APTs. The additional practices increase the depth and sophistication of cybersecurity capabilities.

2.4 CMMC Domains

The CMMC model consists of 17 domains. The majority of these domains originate from the security-related areas in Federal Information Processing Standards (FIPS) Publication 200 [12] and the related security requirement families from NIST SP 800-171 [4]. The CMMC model also includes the three domains of Asset Management (AM), Recovery (RE), and Situational Awareness (SA).

These domains and their abbreviations are shown in Figure 4 below.

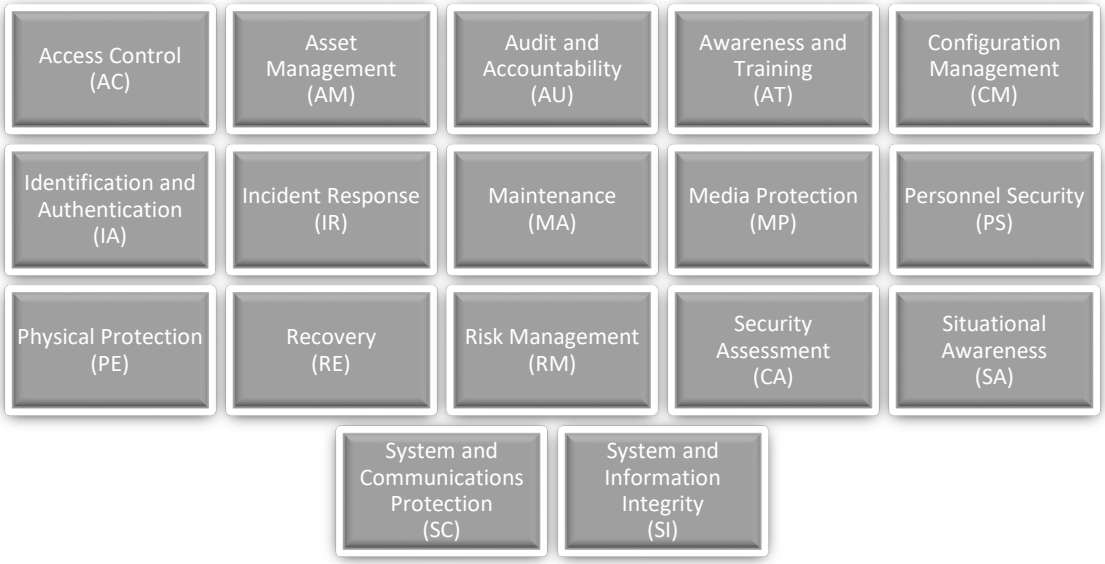

Figure 4. CMMC Domains

2.5 CMMC Capabilities

As previously noted (Figure 1), each domain consists of a set of processes and capabilities (and in turn, practices) across the five levels. Table 1 itemizes the 43 capabilities associated with the 17 domains in the CMMC model.

Table 1. CMMC Capabilities

Domain	Capability
Access Control (AC)	• Establish system access requirements • Control internal system access • Control remote system access • Limit data access to authorized users and processes
Asset Management (AM)	• Identify and document assets
Audit and Accountability (AU)	• Define audit requirements • Perform auditing • Identify and protect audit information • Review and manage audit logs
Awareness and Training (AT)	• Conduct security awareness activities • Conduct training
Configuration Management (CM)	• Establish configuration baselines • Perform configuration and change management
Identification and Authentication (IA)	• Grant access to authenticated entities
Incident Response (IR)	• Plan incident response • Detect and report events • Develop and implement a response to a declared incident • Perform post incident reviews • Test incident response
Maintenance (MA)	• Manage maintenance
Media Protection (MP)	• Identify and mark media • Protect and control media • Sanitize media • Protect media during transport
Personnel Security (PS)	• Screen personnel • Protect CUI during personnel actions
Physical Protection (PE)	• Limit physical access
Recovery (RE)	• Manage back-ups
Risk Management (RM)	• Identify and evaluate risk • Manage risk
Security Assessment (CA)	• Develop and manage a system security plan • Define and manage controls • Perform code reviews
Situational Awareness (SA)	• Implement threat monitoring
Systems and Communications Protection (SC)	• Define security requirements for systems and communications • Control communications at system boundaries
System and Information Integrity (SI)	• Identify and manage information system flaws • Identify malicious content • Perform network and system monitoring • Implement advanced email protections

2.6 CMMC Processes

2.6.1 Background

The term *institutionalization* characterizes the extent to which an activity is embedded or ingrained in the operations of an organization [9,10]. 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 that the outcomes will be consistent, repeatable, and of high quality [9,10].

The CMMC maturity levels serve as a way to measure an organization's process maturity or *process institutionalization*.

2.6.2 Processes

Within the context of the CMMC model, process institutionalization provides additional assurances that the practices associated with each level are implemented effectively. The CMMC model consists of five maturity processes that span Maturity Levels (ML) 2-5 and apply to all domains (Table 2). As previously noted, organizations perform practices at Level 1 but process maturity is not assessed for ML 1.

Table 2. CMMC Processes

Maturity Level	Maturity Level Description	Processes
ML 1	**Performed**	*There are no maturity processes assessed at Maturity Level 1.* *An organization performs Level 1 practices but does not have process institutionalization requirements.*
ML 2	**Documented**	Establish a policy that includes [DOMAIN NAME].
		Document the CMMC practices to implement the [DOMAIN NAME] policy.
ML 3	**Managed**	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
ML 4	**Reviewed**	Review and measure [DOMAIN NAME] activities for effectiveness.
ML 5	**Optimizing**	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

2.7 CMMC Practices

2.7.1 Overview

The CMMC model measures not only process maturity or institutionalization, but also the implementation of practices. The model consists of 171 practices that are mapped across the five levels for all capabilities and domains. This mapping and the cumulative nature of the model is shown in Figure 5.

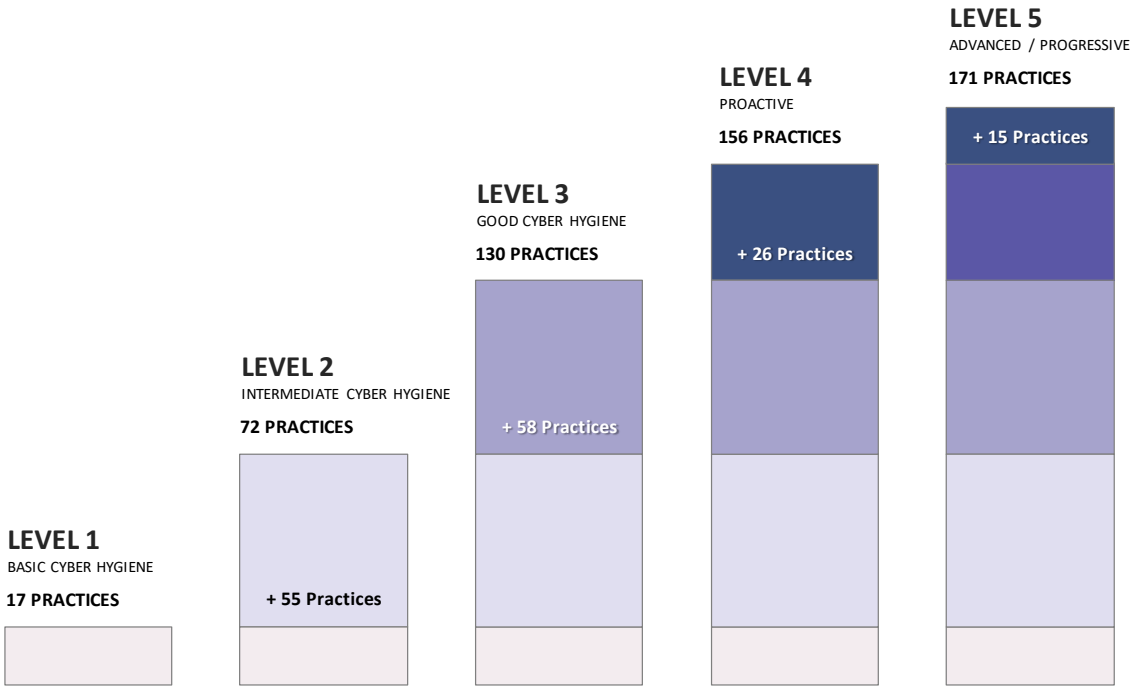

Figure 5. CMMC Practices Per Level

The majority of the practices (110 of 171) originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 [3] and DFARS Clause 252.204-7012 [5], respectively. Although previously noted, the following is restated for emphasis:

- Level 1 is equivalent to all of the safeguarding requirements from FAR Clause 52.204-21.
- Level 3, building on Levels 1 and 2, includes all of the security requirements in NIST SP 800-171 plus other practices.

The remaining practices stem from multiple references as well as inputs from the DIB and DoD stakeholders (Table 3). Due to various considerations, CMMC Levels 4-5 include only a subset of the enhanced security requirements from Draft NIST SP 800-171B [6].

Table 3. Source for CMMC Practices Per Level

CMMC Level	Number of Practices Introduced at CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B	Other
1	17	15*	17*	–	–
2	55	–	48	–	7
3	58	–	45	–	13
4	26	–	–	11	15
5	15	–	–	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.

The distribution of practices across domains per level is shown in Figure 6. The six domains of AC, AU, IR, RM, SC, and SI account for the majority of all practices (105 of 171). The distribution of practices across domains for Levels 4-5 is relatively more uniform than for Levels 1-3.

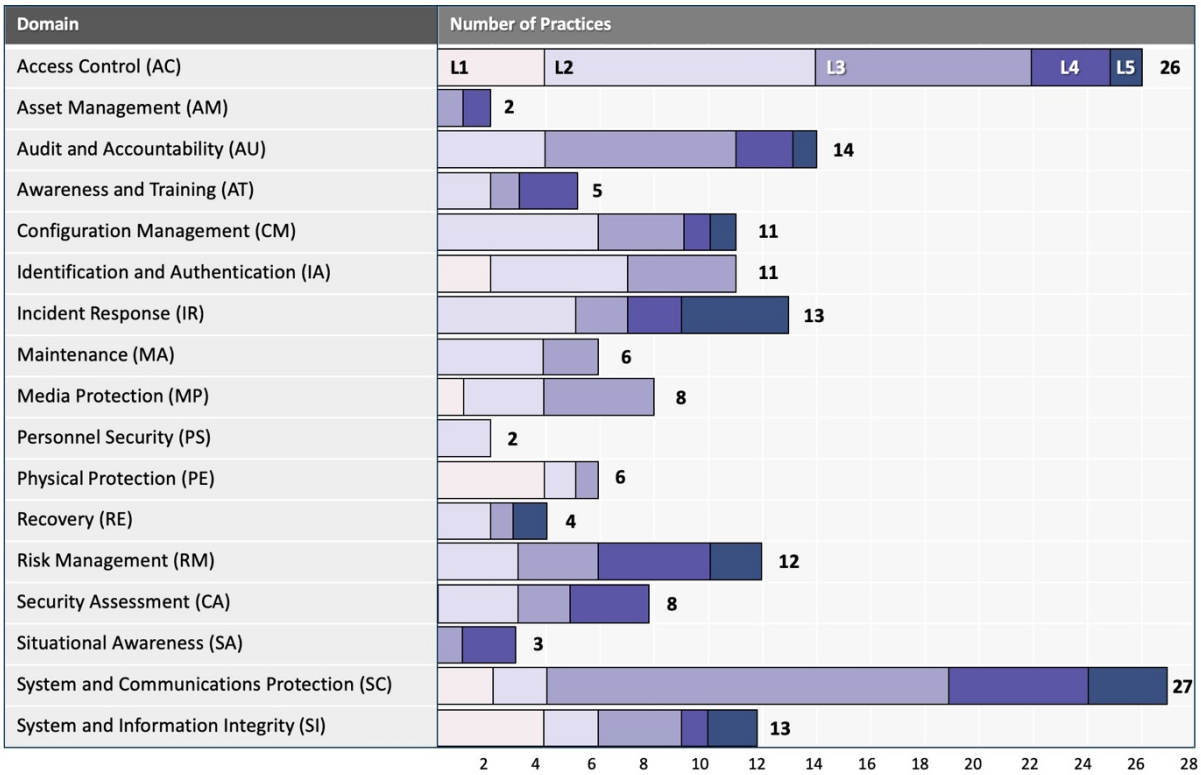

Figure 6. CMMC Practices Across Domains Per Level

2.7.2 List of Practices

This subsection itemizes the practices for each domain and at each level.

Each practice is specified using the convention of [DOMAIN].[LEVEL].[PRACTICE NUMBER] where:

- DOMAIN is the two letter domain abbreviation;
- LEVEL is the level number; and
- PRACTICE NUMBER is the identifier assigned to that practice.

ACCESS CONTROL (AC)

Level 1

AC.1.001	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.1.002	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.1.003	Verify and control/limit connections to and use of external information systems.
AC.1.004	Control information posted or processed on publicly accessible information systems.

Level 2

AC.2.005	Provide privacy and security notices consistent with applicable CUI rules.
AC.2.006	Limit use of portable storage devices on external systems.
AC.2.007	Employ the principle of least privilege, including for specific security functions and privileged accounts.
AC.2.008	Use non-privileged accounts or roles when accessing nonsecurity functions.
AC.2.009	Limit unsuccessful logon attempts.
AC.2.010	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
AC.2.011	Authorize wireless access prior to allowing such connections.
AC.2.013	Monitor and control remote access sessions.
AC.2.015	Route remote access via managed access control points.
AC.2.016	Control the flow of CUI in accordance with approved authorizations.

Level 3

AC.3.017	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
AC.3.018	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
AC.3.019	Terminate (automatically) user sessions after a defined condition.

AC.3.012 Protect wireless access using authentication and encryption.

AC.3.020 Control connection of mobile devices.

AC.3.014 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

AC.3.021 Authorize remote execution of privileged commands and remote access to security-relevant information.

AC.3.022 Encrypt CUI on mobile devices and mobile computing platforms.

Level 4

AC.4.023 Control information flows between security domains on connected systems.

AC.4.025 Periodically review and update CUI program access permissions.

AC.4.032 Restrict remote network access based on organizationally defined risk factors such as time of day, location of access, physical location, network connection state, and measured properties of the current user and role.

Level 5

AC.5.024 Identify and mitigate risk associated with unidentified wireless access points connected to the network.

ASSET MANAGEMENT (AM)

Level 3

AM.3.036 Define procedures for the handling of CUI data.

Level 4

AM.4.226 Employ a capability to discover and identify systems with specific component attributes (e.g., firmware level, OS type) within your inventory.

AUDIT AND ACCOUNTABILITY (AU)

Level 2

AU.2.041 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.

AU.2.042 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

AU.2.043 Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

AU.2.044 Review audit logs.

Level 3

AU.3.045 Review and update logged events.

AU.3.046 Alert in the event of an audit logging process failure.

AU.3.048 Collect audit information (e.g., logs) into one or more central repositories.

AU.3.049 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

AU.3.050 Limit management of audit logging functionality to a subset of privileged users.

AU.3.051 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

AU.3.052 Provide audit record reduction and report generation to support on-demand analysis and reporting.

Level 4

AU.4.053 Automate analysis of audit logs to identify and act on critical indicators (TTPs) and/or organizationally defined suspicious activity.

AU.4.054 Review audit information for broad activity in addition to per-machine activity.

Level 5

AU.5.055 Identify assets not reporting audit logs and assure appropriate organizationally defined systems are logging.

AWARENESS AND TRAINING (AT)

Level 2

AT.2.056 Ensure that managers, system administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

AT.2.057 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.

Level 3

AT.3.058 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Level 4

AT.4.059 Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.

AT.4.060 Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training.

CONFIGURATION MANAGEMENT (CM)

Level 2

CM.2.061 Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

CM.2.062 Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

CM.2.063 Control and monitor user-installed software.

CM.2.064 Establish and enforce security configuration settings for information technology products employed in organizational systems.

CM.2.065 Track, review, approve, or disapprove, and log changes to organizational systems.

CM.2.066 Analyze the security impact of changes prior to implementation.

Level 3

CM.3.067 Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

CM.3.068 Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

CM.3.069 Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.

Level 4

CM.4.073 Employ application whitelisting and an application vetting process for systems identified by the organization.

Level 5

CM.5.074 Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).

IDENTIFICATION AND AUTHENTICATION (IA)

Level 1

IA.1.076 Identify information system users, processes acting on behalf of users, or devices.

IA.1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Level 2

IA.2.078 Enforce a minimum password complexity and change of characters when new passwords are created.

IA.2.079 Prohibit password reuse for a specified number of generations.

IA.2.080 Allow temporary password use for system logons with an immediate change to a permanent password.

IA.2.081 Store and transmit only cryptographically-protected passwords.

IA.2.082 Obscure feedback of authentication information.

Level 3

IA.3.083 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

IA.3.084 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

IA.3.085 Prevent the reuse of identifiers for a defined period.

IA.3.086 Disable identifiers after a defined period of inactivity.

INCIDENT RESPONSE (IR)

Level 2

IR.2.092 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.

IR.2.093 Detect and report events.

IR.2.094 Analyze and triage events to support event resolution and incident declaration.

IR.2.096 Develop and implement responses to declared incidents according to pre-defined procedures.

IR.2.097 Perform root cause analysis on incidents to determine underlying causes.

Level 3

IR.3.098 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.

IR.3.099 Test the organizational incident response capability.

Level 4

IR.4.100 Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.

IR.4.101 Establish and maintain a security operations center capability that facilitates a 24/7 response capability.

Level 5

IR.5.106 In response to cyber incidents, utilize forensic data gathering across impacted systems, ensuring the secure transfer and protection of forensic data.

IR.5.102 Use a combination of manual and automated, real-time responses to anomalous activities that match incident patterns.

IR.5.108 Establish and maintain a cyber incident response team that can investigate an issue physically or virtually at any location within 24 hours.

IR.5.110 Perform unannounced operational exercises to demonstrate technical and procedural responses.

MAINTENANCE (MA)

Level 2

MA.2.111 Perform maintenance on organizational systems.

MA.2.112 Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.

MA.2.113 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

MA.2.114 Supervise the maintenance activities of personnel without required access authorization.

Level 3

MA.3.115 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

MA.3.116 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

MEDIA PROTECTION (MP)

Level 1

MP.1.118 Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Level 2

MP.2.119 Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.

MP.2.120 Limit access to CUI on system media to authorized users.

MP.2.121 Control the use of removable media on system components.

Level 3

MP.3.122 Mark media with necessary CUI markings and distribution limitations.

MP.3.123 Prohibit the use of portable storage devices when such devices have no identifiable owner.

MP.3.124 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

MP.3.125 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

PERSONNEL SECURITY (PS)

Level 2

PS.2.127 Screen individuals prior to authorizing access to organizational systems containing CUI.

PS.2.128 Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

PHYSICAL PROTECTION (PE)

Level 1

PE.1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

PE.1.132 Escort visitors and monitor visitor activity.

PE.1.133 Maintain audit logs of physical access.

PE.1.134 Control and manage physical access devices.

Level 2

PE.2.135 Protect and monitor the physical facility and support infrastructure for organizational systems.

Level 3

PE.3.136 Enforce safeguarding measures for CUI at alternate work sites.

RECOVERY (RE)

Level 2

RE.2.137 Regularly perform and test data back-ups.

RE.2.138 Protect the confidentiality of backup CUI at storage locations.

Level 3

RE.3.139 Regularly perform complete, comprehensive, and resilient data back-ups as organizationally defined.

Level 5

RE.5.140 Ensure information processing facilities meet organizationally defined information security continuity, redundancy, and availability requirements.

RISK MANAGEMENT (RM)

Level 2

RM.2.141 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.

RM.2.142 Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

RM.2.143 Remediate vulnerabilities in accordance with risk assessments.

Level 3

RM.3.144 Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.

RM.3.146 Develop and implement risk mitigation plans.

RM.3.147 Manage non-vendor-supported products (e.g., end of life) separately and restrict as necessary to reduce risk.

Level 4

RM.4.149 Catalog and periodically update threat profiles and adversary TTPs.

RM.4.150 Employ threat intelligence to inform the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.

RM.4.151 Perform scans for unauthorized ports available across perimeter network boundaries over the organization's Internet network boundaries and other organizationally defined boundaries.

RM.4.148 Develop and update as required, a plan for managing supply chain risks associated with the IT supply chain.

Level 5

RM.5.152 Utilize an exception process for non-whitelisted software that includes mitigation techniques.

RM.5.155 Analyze the effectiveness of security solutions at least annually to address anticipated risk to the system and the organization based on current and accumulated threat intelligence.

SECURITY ASSESSMENT (CA)

Level 2

CA.2.157 Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

CA.2.158 Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

CA.2.159 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

Level 3

CA.3.161 Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA.3.162 Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk.

Level 4

CA.4.163 Create, maintain, and leverage a security strategy and roadmap for organizational cybersecurity improvement.

CA.4.164 Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts.

CA.4.227 Periodically perform red teaming against organizational assets in order to validate defensive capabilities.

SITUATIONAL AWARENESS (SA)

Level 3

SA.3.169 Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.

Level 4

SA.4.171 Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.

SA.4.173 Design network and system security capabilities to leverage, integrate, and share indicators of compromise.

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Level 1

SC.1.175 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

SC.1.176 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Level 2

SC.2.178 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

SC.2.179 Use encrypted sessions for the management of network devices.

Level 3

SC.3.177 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

SC.3.180 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

SC.3.181 Separate user functionality from system management functionality.

SC.3.182 Prevent unauthorized and unintended information transfer via shared system resources.

SC.3.183 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

SC.3.184 Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).

SC.3.185 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

SC.3.186 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

SC.3.187 Establish and manage cryptographic keys for cryptography employed in organizational systems.

SC.3.188 Control and monitor the use of mobile code.

SC.3.189 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

SC.3.190 Protect the authenticity of communications sessions.

SC.3.191 Protect the confidentiality of CUI at rest.

SC.3.192 Implement Domain Name System (DNS) filtering services.

SC.3.193 Implement a policy restricting the publication of CUI on externally owned, publicly accessible websites (e.g., forums, LinkedIn, Facebook, Twitter).

Level 4

SC.4.197 Employ physical and logical isolation techniques in the system and security architecture and/or where deemed appropriate by the organization.

SC.4.228 Isolate administration of organizationally defined high-value critical network infrastructure components and servers.

SC.4.199 Utilize threat intelligence to proactively block DNS requests from reaching malicious domains.

SC.4.202 Employ mechanisms to analyze executable code and scripts (e.g., sandbox) traversing Internet network boundaries or other organizationally defined boundaries.

SC.4.229 Utilize a URL categorization service and implement techniques to enforce URL filtering of websites that are not approved by the organization.

Level 5

SC.5.198 Configure monitoring systems to record packets passing through the organization's Internet network boundaries and other organizationally defined boundaries.

SC.5.230 Enforce port and protocol compliance.

SC.5.208 Employ organizationally defined and tailored boundary protections in addition to commercially available solutions.

SYSTEM AND INFORMATION INTEGRITY (SI)

Level 1

SI.1.210 Identify, report, and correct information and information system flaws in a timely manner.

SI.1.211 Provide protection from malicious code at appropriate locations within organizational information systems.

SI.1.212 Update malicious code protection mechanisms when new releases are available.

SI.1.213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Level 2

SI.2.214 Monitor system security alerts and advisories and take action in response.

SI.2.216 Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

SI.2.217 Identify unauthorized use of organizational systems.

Level 3

SI.3.218 Employ spam protection mechanisms at information system access entry and exit points.

SI.3.219 Implement email forgery protections.

SI.3.220 Utilize sandboxing to detect or block potentially malicious email.

Level 4

SI.4.221 Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.

Level 5

SI.5.222 Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.

SI.5.223 Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.

3. Summary

The Cybersecurity Maturity Model Certification (CMMC) framework contains five maturity processes and 171 cybersecurity best practices progressing across five maturity levels. The CMMC maturity processes institutionalize cybersecurity activities to ensure they are consistent, repeatable, and of high quality. The CMMC practices provide a range of mitigation across the levels, starting with basic safeguarding at Level 1, moving to the broad protection of Controlled Unclassified Information (CUI) at Level 3, and culminating with reducing the risk from Advanced Persistent Threats (APTs) at Levels 4 and 5. The CMMC framework is coupled with a certification program to verify the implementation of processes and practices.

Created in collaboration with a community of Department of Defense (DoD) stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the Defense Industrial Base (DIB) sector, the CMMC framework addresses the needs of the DoD to protect its unclassified information (i.e., Federal Contract Information (FCI) and CUI) during the acquisition and sustainment of products and services from the DIB. This model represents one of multiple lines of effort that the Department and industry are pursuing to enhance the security and resiliency of the DIB sector. These efforts are instrumental in establishing cybersecurity as a foundation for future DoD acquisitions.


OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT
CYBERSECURITY MATURITY MODEL
CERTIFICATION