Cybersecurity Maturity Model Certification (CMMC) Model Overview

Version 2.0 | December 2021

NOTICES

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.

TABLE OF CONTENTS

1. Introduction

The theft of intellectual property and sensitive information from all industrial sectors because of 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 more than 300,000 companies that support the warfighter and contribute toward 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 undercuts U.S. technical advantages and innovation as well as significantly increases risk to national security.

As part of multiple lines of effort focused on the security 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].

To 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. 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 Revision (Rev) 2 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 [3, 4, 5]. DFARS clause 252.204-7012

[5] specifies additional requirements beyond the NIST SP 800-171 security requirements, such as incident reporting. CMMC is designed to provide 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 the CMMC model, a DIB contractor can achieve a specific CMMC level for its entire enterprise network or for a particular segment(s) or enclave(s), depending on where the information to be protected is handled and stored.

1.1 Document Organization

Section 2 presents the CMMC model and each of its elements in detail. Appendix A provides the model as a matrix. Appendix B maps the CMMC model to other secondary sources. Appendix C lists the abbreviations and acronyms. Finally, Appendix D provides the references contained in this document.

1.2 Supporting Documents

This document is supported by multiple companion documents that provide additional information. *CMMC Assessment Guides* present assessment objectives, discussion, examples, potential assessment considerations, and key references for each practice. The *CMMC Glossary and Acronyms* defines terms. The *CMMC Errata* document lists known errata in the CMMC documentation and the version in which the correction was, or will be, made.

2. CMMC Model

2.1 Overview

The CMMC framework consists of the security requirements from NIST SP 800-171 Rev 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* and a subset of the requirements from NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*. The model framework organizes these practices into a set of domains, which map directly to the NIST SP 800-171 Rev 2 families. There are three levels within CMMC—Level 1, Level 2, and Level 3—as described in the sections below.

2.2 CMMC Levels

2.2.1 Descriptions

The CMMC model measures the implementation of cybersecurity requirements at three levels. Each level consists of a set of CMMC practices:

- Level 1: Encompasses the *basic safeguarding requirements* for FCI specified in FAR Clause 52.204-21.
- Level 2: Encompasses the *security requirements* for CUI specified in NIST SP 800-171 Rev 2 per DFARS Clause 252.204-7012 [3, 4, 5].
- Level 3: Information on Level 3 will be released at a later date and will contain a subset of the *security requirements* specified in NIST SP 800-172 [6].

The CMMC levels and associated sets of practices across domains are cumulative. More specifically, for an organization to achieve a specific CMMC level, it must also demonstrate achievement of the preceding lower levels. For the case in which an organization does not meet its targeted level, it will be certified at the highest level for which it has achieved all applicable practices.

2.2.2 CMMC 2.0 Overview

Figure 1 provides an overview of the CMMC 2.0 Levels.

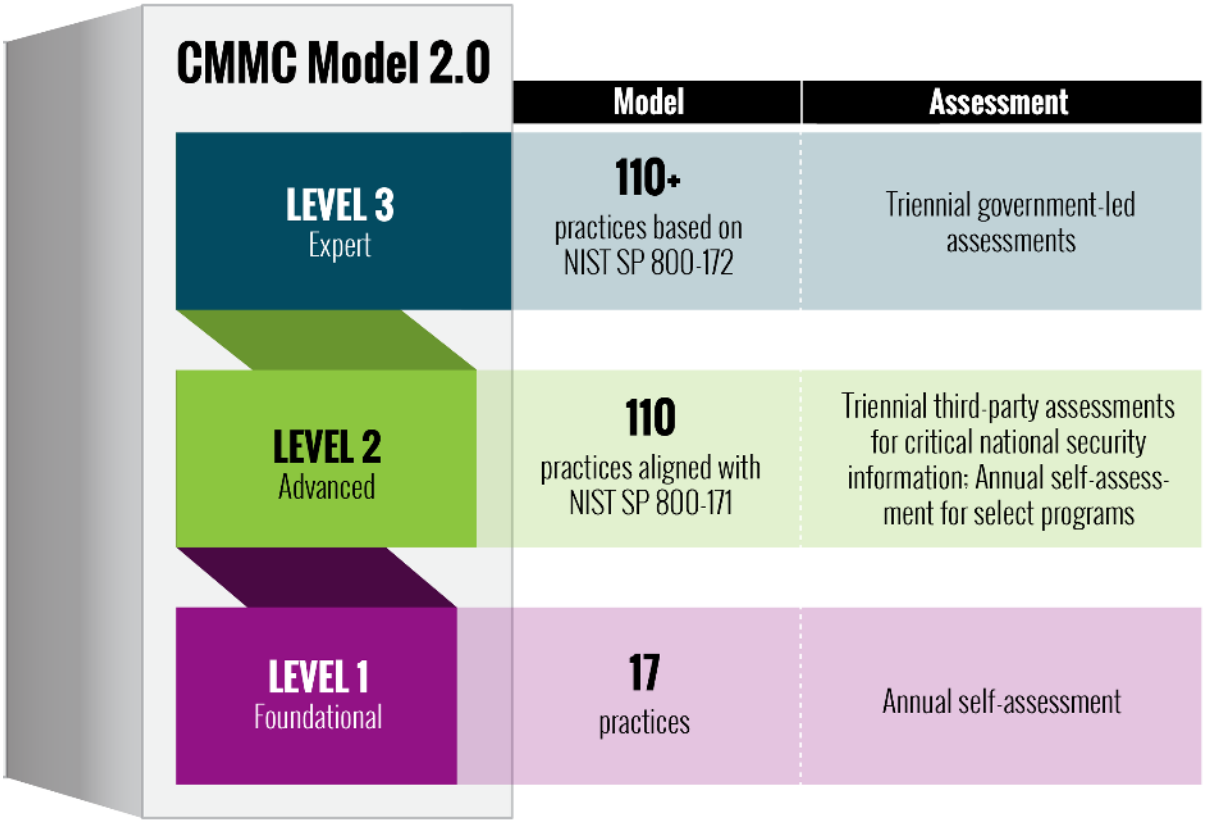

Figure 1. CMMC 2.0 Level Overview

2.2.3 CMMC Level 1

Level 1 focuses on the protection of FCI and consists of only practices that correspond to the basic safeguarding requirements specified in 48 CFR 52.204-21, commonly referred to as the FAR Clause [3].

2.2.4 CMMC Level 2

- Practices: Advanced

Level 2 focuses on the protection of CUI and encompasses the 110 security requirements specified in NIST SP 800-171 Rev 2 [4].

2.2.5 CMMC Level 3

- Practices: Expert

  Level 3 will be based on a subset of NIST SP 800-172 requirements [6]. Details will be released at a later date.

2.3 CMMC Domains

The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171. These domains and their abbreviations are as follows:

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Configuration Management (CM)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

2.4 CMMC Practices

2.4.1 Overview

The CMMC model measures the implementation of the NIST SP 800-171 Rev 2 [4] security requirements. The practices originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 [3] and DFARS Clause 252.204-7012 [5], respectively.

- Level 1 is equivalent to all of the safeguarding requirements from FAR Clause 52.204-21.
- Level 2 is equivalent to all of the security requirements in NIST SP 800-171 Revision 2.
- Level 3 will be based on a subset of NIST SP 800-172 and more detailed information will be released at a later date.

2.4.2 List of Practices

This subsection itemizes the practices for each domain and at each level. Each practice has a practice identification number in the format – **DD.L#-REQ** – where:

- DD is the two-letter domain abbreviation;
- L# is the level number; and
- REQ is the NIST SP 800-171 Rev 2 or NIST SP 800-172 security requirement number.

Below the identification number, a short name identifier is provided for each practice, meant to be used for quick reference only. Finally, each practice has a complete practice statement.

ACCESS CONTROL (AC)

Level 1

AC.L1-3.1.1 *Authorized Access Control*	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.L1-3.1.2 *Transaction & Function Control*	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.L1-3.1.20 *External Connections*	Verify and control/limit connections to and use of external information systems.
AC.L1-3.1.22 *Control Public Information*	Control information posted or processed on publicly accessible information systems.

Level 2

AC.L2-3.1.3 *Control CUI Flow*	Control the flow of CUI in accordance with approved authorizations.
AC.L2-3.1.4 *Separation of Duties*	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
AC.L2-3.1.5 *Least Privilege*	Employ the principle of least privilege, including for specific security functions and privileged accounts.
AC.L2-3.1.6 *Non-Privileged Account Use*	Use non-privileged accounts or roles when accessing nonsecurity functions.
AC.L2-3.1.7 *Privileged Functions*	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.
AC.L2-3.1.8 *Unsuccessful Logon Attempts*	Limit unsuccessful logon attempts.
AC.L2-3.1.9 *Privacy & Security Notices*	Provide privacy and security notices consistent with applicable CUI rules.
AC.L2-3.1.10 *Session Lock*	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.
AC.L2-3.1.11 *Session Termination*	Terminate (automatically) a user session after a defined condition.
AC.L2-3.1.12 *Control Remote Access*	Monitor and control remote access sessions.
AC.L2-3.1.13 *Remote Access Confidentiality*	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
AC.L2-3.1.14 *Remote Access Routing*	Route remote access via managed access control points.
AC.L2-3.1.15 *Privileged Remote Access*	Authorize remote execution of privileged commands and remote access to security-relevant information.
AC.L2-3.1.16 *Wireless Access Authorization*	Authorize wireless access prior to allowing such connections.
AC.L2-3.1.17 *Wireless Access Protection*	Protect wireless access using authentication and encryption.
AC.L2-3.1.18 *Mobile Device Connection*	Control connection of mobile devices.
AC.L2-3.1.19 *Encrypt CUI on Mobile*	Encrypt CUI on mobile devices and mobile computing platforms.
AC.L2-3.1.21 *Portable Storage Use*	Limit use of portable storage devices on external systems.

Level 3

TBD

AWARENESS AND TRAINING (AT)

Level 2

AT.L2-3.2.1 *Role-Based Risk Awareness*	Ensure that managers, systems 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.L2-3.2.2 *Role-Based Training*	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
AT.L2-3.2.3 *Insider Threat Awareness*	Provide security awareness training on recognizing and reporting potential indicators of insider threat.

Level 3

TBD

AUDIT AND ACCOUNTABILITY (AU)

Level 2

AU.L2-3.3.1 *System Auditing*	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.L2-3.3.2 *User Accountability*	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.L2-3.3.3 *Event Review*	Review and update logged events.
AU.L2-3.3.4 *Audit Failure Alerting*	Alert in the event of an audit logging process failure.
AU.L2-3.3.5 *Audit Correlation*	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
AU.L2-3.3.6 *Reduction & Reporting*	Provide audit record reduction and report generation to support on-demand analysis and reporting.
AU.L2-3.3.7 *Authoritative Time Source*	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

AU.L2-3.3.8
Audit Protection
Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

AU.L2-3.3.9
Audit Management
Limit management of audit logging functionality to a subset of privileged users.

Level 3

TBD

CONFIGURATION MANAGEMENT (CM)

Level 2

CM.L2-3.4.1
System Baselining
Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

CM.L2-3.4.2
Security Configuration Enforcement
Establish and enforce security configuration settings for information technology products employed in organizational systems.

CM.L2-3.4.3
System Change Management
Track, review, approve or disapprove, and log changes to organizational systems.

CM.L2-3.4.4
Security Impact Analysis
Analyze the security impact of changes prior to implementation.

CM.L2-3.4.5
Access Restrictions for Change
Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.

CM.L2-3.4.6
Least Functionality
Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.

CM.L2-3.4.7
Nonessential Functionality
Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.

CM.L2-3.4.8
Application Execution Policy
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.

CM.L2-3.4.9
User-Installed Software
Control and monitor user-installed software.

Level 3

TBD

IDENTIFICATION AND AUTHENTICATION (IA)

Level 1

IA.L1-3.5.1
Identification
Identify information system users, processes acting on behalf of users, or devices.

IA.L1-3.5.2 *Authentication*	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Level 2

IA.L2-3.5.3 *Multifactor Authentication*	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
IA.L2-3.5.4 *Replay-Resistant Authentication*	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
IA.L2-3.5.5 *Identifier Reuse*	Prevent reuse of identifiers for a defined period.
IA.L2-3.5.6 *Identifier Handling*	Disable identifiers after a defined period of inactivity.
IA.L2-3.5.7 *Password Complexity*	Enforce a minimum password complexity and change of characters when new passwords are created.
IA.L2-3.5.8 *Password Reuse*	Prohibit password reuse for a specified number of generations.
IA.L2-3.5.9 *Temporary Passwords*	Allow temporary password use for system logons with an immediate change to a permanent password.
IA.L2-3.5.10 *Cryptographically-Protected Passwords*	Store and transmit only cryptographically protected passwords.
IA.L2-3.5.11 *Obscure Feedback*	Obscure feedback of authentication information.

Level 3

TBD

INCIDENT RESPONSE (IR)

Level 2

IR.L2-3.6.1 *Incident Handling*	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.
IR.L2-3.6.2 *Incident Reporting*	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
IR.L2-3.6.3 *Incident Response Testing*	Test the organizational incident response capability.

Level 3

TBD

MAINTENANCE (MA)

Level 2

MA.L2-3.7.1 *Perform Maintenance*	Perform maintenance on organizational systems.
MA.L2-3.7.2 *System Maintenance Control*	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.
MA.L2-3.7.3 *Equipment Sanitization*	Ensure equipment removed for off-site maintenance is sanitized of any CUI.
MA.L2-3.7.4 *Media Inspection*	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.
MA.L2-3.7.5 *Nonlocal Maintenance*	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.
MA.L2-3.7.6 *Maintenance Personnel*	Supervise the maintenance activities of maintenance personnel without required access authorization.

Level 3

TBD

MEDIA PROTECTION (MP)

Level 1

MP.L1-3.8.3 *Media Disposal*	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Level 2

MP.L2-3.8.1 *Media Protection*	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.
MP.L2-3.8.2 *Media Access*	Limit access to CUI on system media to authorized users.
MP.L2-3.8.4 *Media Markings*	Mark media with necessary CUI markings and distribution limitations.
MP.L2-3.8.5 *Media Accountability*	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.
MP.L2-3.8.6 *Portable Storage Encryption*	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
MP.L2-3.8.7 *Removable Media*	Control the use of removable media on system components.

MP.L2-3.8.8
Shared Media
Prohibit the use of portable storage devices when such devices have no identifiable owner.

MP.L2-3.8.9
Protect Backups
Protect the confidentiality of backup CUI at storage locations.

Level 3

TBD

PERSONNEL SECURITY (PS)

Level 2

PS.L2-3.9.1
Screen Individuals
Screen individuals prior to authorizing access to organizational systems containing CUI.

PS.L2-3.9.2
Personnel Actions
Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

PHYSICAL PROTECTION (PE)

Level 1

PE.L1-3.10.1
Limit Physical Access
Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

PE.L1-3.10.3
Escort Visitors
Escort visitors and monitor visitor activity.

PE.L1-3.10.4
Physical Access Logs
Maintain audit logs of physical access.

PE.L1-3.10.5
Manage Physical Access
Control and manage physical access devices.

Level 2

PE.L2-3.10.2
Monitor Facility
Protect and monitor the physical facility and support infrastructure for organizational systems.

PE.L2-3.10.6
Alternative Work Sites
Enforce safeguarding measures for CUI at alternate work sites.

Level 3

TBD

RISK ASSESSMENT (RA)

Level 2

RA.L2-3.11.1 *Risk Assessments*	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.
RA.L2-3.11.2 *Vulnerability Scan*	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
RA.L2-3.11.3 *Vulnerability Remediation*	Remediate vulnerabilities in accordance with risk assessments.

Level 3

TBD

SECURITY ASSESSMENT (CA)

Level 2

CA.L2-3.12.1 *Security Control Assessment*	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.
CA.L2-3.12.2 *Plan of Action*	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.
CA.L2-3.12.3 *Security Control Monitoring*	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.
CA.L2-3.12.4 *System Security Plan*	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.

Level 3

TBD

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Level 1

SC.L1-3.13.1 *Boundary Protection*	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.L1-3.13.5 *Public-Access System Separation*	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Level 2

SC.L2-3.13.2 *Security Engineering*	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.
SC.L2-3.13.3 *Role Separation*	Separate user functionality from system management functionality.
SC.L2-3.13.4 *Shared Resource Control*	Prevent unauthorized and unintended information transfer via shared system resources.
SC.L2-3.13.6 *Network Communication by Exception*	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).
SC.L2-3.13.7 *Split Tunneling*	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.L2-3.13.8 *Data in Transit*	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
SC.L2-3.13.9 *Connections Termination*	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.
SC.L2-3.13.10 *Key Management*	Establish and manage cryptographic keys for cryptography employed in organizational systems.
SC.L2-3.13.11 *CUI Encryption*	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
SC.L2-3.13.12 *Collaborative Device Control*	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.
SC.L2-3.13.13 *Mobile Code*	Control and monitor the use of mobile code.
SC.L2-3.13.14 *Voice over Internet Protocol*	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.
SC.L2-3.13.15 *Communications Authenticity*	Protect the authenticity of communications sessions.
SC.L2-3.13.16 *Data at Rest*	Protect the confidentiality of CUI at rest.

Level 3

TBD

SYSTEM AND INFORMATION INTEGRITY (SI)

Level 1

SI.L1-3.14.1 *Flaw Remediation*	Identify, report, and correct information and information system flaws in a timely manner.
SI.L1-3.14.2 *Malicious Code Protection*	Provide protection from malicious code at appropriate locations within organizational information systems.
SI.L1-3.14.4 *Update Malicious Code Protection*	Update malicious code protection mechanisms when new releases are available.
SI.L1-3.14.5 *System & File Scanning*	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.L2-3.14.3 *Security Alerts & Advisories*	Monitor system security alerts and advisories and take action in response.
SI.L2-3.14.6 *Monitor Communications for Attacks*	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.
SI.L2-3.14.7 *Identify Unauthorized Use*	Identify unauthorized use of organizational systems.

Level 3

TBD

3. Summary

The CMMC framework contains three levels. The CMMC practices provide threat mitigation across the levels, starting with basic safeguarding of FCI at Level 1, moving to the broad protection of CUI at Level 2, and culminating with reducing the risk from Advanced Persistent Threats (APTs) at Level 3. The CMMC framework is coupled with a certification program to verify the implementation of practices.

Created in collaboration with a community of DoD stakeholders, UARCs, FFRDCs, and the DIB sector, the CMMC framework addresses the needs of the DoD to protect its unclassified information during the acquisition and sustainment of products and services from the DIB. This model represents one of multiple lines of effort that the DoD and industry are pursuing to enhance the security of the DIB sector. These efforts are instrumental in establishing cybersecurity as a foundation for future DoD acquisitions.

Appendix A. CMMC Model Matrix

This appendix presents the model in matrix form by domain. The three columns list the associated practices for each CMMC level.

Each practice is contained in a single cell. The practice identification number is bolded at the top of each cell. The next line contains the practice short name identifier, in italics, which is meant to be used for quick reference only. Below the short name is the complete CMMC practice statement. Finally, the bulleted list at the bottom contains the FAR Clause 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172 reference as appropriate.

ACCESS CONTROL (AC)

Level 1	Level 2	Level 3 (TBD)
AC.L1-3.1.1 *Authorized Access Control* Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 Rev 2 3.1.1	**AC.L2-3.1.3** *Control CUI Flow* Control the flow of CUI in accordance with approved authorizations. • NIST SP 800-171 Rev 2 3.1.3	
AC.L1-3.1.2 *Transaction & Function Control* Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 Rev 2 3.1.2	**AC.L2-3.1.4** *Separation of Duties* Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 Rev 2 3.1.4	
AC.L1-3.1.20 *External Connections* Verify and control/limit connections to and use of external information systems. • FAR Clause 52.204-21 b.1.iii • NIST SP 800-171 Rev 2 3.1.20	**AC.L2-3.1.5** *Least Privilege* Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 Rev 2 3.1.5	
AC.L1-3.1.22 *Control Public Information* Control information posted or processed on publicly accessible information systems. • FAR Clause 52.204-21 b.1.iv • NIST SP 800-171 Rev 2 3.1.22	**AC.L2-3.1.6** *Non-Privileged Account Use* Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 Rev 2 3.1.6	
	AC.L2-3.1.7 *Privileged Functions* Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 Rev 2 3.1.7	
	AC.L2-3.1.8 *Unsuccessful Logon Attempts* Limit unsuccessful logon attempts. • NIST SP 800-171 Rev 2 3.1.8	
	AC.L2-3.1.9 *Privacy & Security Notices* Provide privacy and security notices consistent with applicable CUI rules. • NIST SP 800-171 Rev 2 3.1.9	
	AC.L2-3.1.10 *Session Lock* Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 Rev 2 3.1.10	
	AC.L2-3.1.11 *Session Termination* Terminate (automatically) a user session after a defined condition. • NIST SP 800-171 Rev 2 3.1.11	

Level 1	Level 2	Level 3 (TBD)
	AC.L2-3.1.12 *Control Remote Access* Monitor and control remote access sessions. • NIST SP 800-171 Rev 2 3.1.12	
	AC.L2-3.1.13 *Remote Access Confidentiality* Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. • NIST SP 800-171 Rev 2 3.1.13	
	AC.L2-3.1.14 *Remote Access Routing* Route remote access via managed access control points. • NIST SP 800-171 Rev 2 3.1.14	
	AC.L2-3.1.15 *Privileged Remote Access* Authorize remote execution of privileged commands and remote access to security-relevant information. • NIST SP 800-171 Rev 2 3.1.15	
	AC.L2-3.1.16 *Wireless Access Authorization* Authorize wireless access prior to allowing such connections. • NIST SP 800-171 Rev 2 3.1.16	
	AC.L2-3.1.17 *Wireless Access Protection* Protect wireless access using authentication and encryption. • NIST SP 800-171 Rev 2 3.1.17	
	AC.L2-3.1.18 *Mobile Device Connection* Control connection of mobile devices. • NIST SP 800-171 Rev 2 3.1.18	
	AC.L2-3.1.19 *Encrypt CUI on Mobile* Encrypt CUI on mobile devices and mobile computing platforms. • NIST SP 800-171 Rev 2 3.1.19	
	AC.L2-3.1.21 *Portable Storage Use* Limit use of portable storage devices on external systems. • NIST SP 800-171 Rev 2 3.1.21	

AWARENESS AND TRAINING (AT)

Level 1	Level 2	Level 3 (TBD)
	AT.L2-3.2.1 *Role-Based Risk Awareness* Ensure that managers, systems 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. • NIST SP 800-171 Rev 2 3.2.1	
	AT.L2-3.2.2 *Role-Based Training* Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities. • NIST SP 800-171 Rev 2 3.2.2	
	AT.L2-3.2.3 *Insider Threat Awareness* Provide security awareness training on recognizing and reporting potential indicators of insider threat. • NIST SP 800-171 Rev 2 3.2.3	

AUDIT AND ACCOUNTABILITY (AU)

Level 1	Level 2	Level 3 (TBD)
	AU.L2-3.3.1 *System Auditing* 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. • NIST SP 800-171 Rev 2 3.3.1	
	AU.L2-3.3.2 *User Accountability* Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions. • NIST SP 800-171 Rev 2 3.3.2	
	AU.L2-3.3.3 *Event Review* Review and update logged events. • NIST SP 800-171 Rev 2 3.3.3	
	AU.L2-3.3.4 *Audit Failure Alerting* Alert in the event of an audit logging process failure. • NIST SP 800-171 Rev 2 3.3.4	
	AU.L2-3.3.5 *Audit Correlation* Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity. • NIST SP 800-171 Rev 2 3.3.5	
	AU.L2-3.3.6 *Reduction & Reporting* Provide audit record reduction and report generation to support on-demand analysis and reporting. • NIST SP 800-171 Rev 2 3.3.6	
	AU.L2-3.3.7 *Authoritative Time Source* Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records. • NIST SP 800-171 Rev 2 3.3.7	
	AU.L2-3.3.8 *Audit Protection* Protect audit information and audit logging tools from unauthorized access, modification, and deletion. • NIST SP 800-171 Rev 2 3.3.8	
	AU.L2-3.3.9 *Audit Management* Limit management of audit logging functionality to a subset of privileged users. • NIST SP 800-171 Rev 2 3.3.9	

CONFIGURATION MANAGEMENT (CM)

Level 1	Level 2	Level 3 (TBD)
	CM.L2-3.4.1 *System Baselining* Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. • NIST SP 800-171 Rev 2 3.4.1	
	CM.L2-3.4.2 *Security Configuration Enforcement* Establish and enforce security configuration settings for information technology products employed in organizational systems. • NIST SP 800-171 Rev 2 3.4.2	
	CM.L2-3.4.3 *System Change Management* Track, review, approve or disapprove, and log changes to organizational systems. • NIST SP 800-171 Rev 2 3.4.3	
	CM.L2-3.4.4 *Security Impact Analysis* Analyze the security impact of changes prior to implementation. • NIST SP 800-171 Rev 2 3.4.4	
	CM.L2-3.4.5 *Access Restrictions for Change* Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems. • NIST SP 800-171 Rev 2 3.4.5	
	CM.L2-3.4.6 *Least Functionality* Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities. • NIST SP 800-171 Rev 2 3.4.6	
	CM.L2-3.4.7 *Nonessential Functionality* Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services. • NIST SP 800-171 Rev 2 3.4.7	
	CM.L2-3.4.8 *Application Execution Policy* 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. • NIST SP 800-171 Rev 2 3.4.8	
	CM.L2-3.4.9 *User-Installed Software* Control and monitor user-installed software. • NIST SP 800-171 Rev 2 3.4.9	

IDENTIFICATION AND AUTHENTICATION (IA)

Level 1	Level 2	Level 3 (TBD)
IA.L1-3.5.1 *Identification* Identify information system users, processes acting on behalf of users, or devices. • FAR Clause 52.204-21 b.1.v • NIST SP 800-171 Rev 2 3.5.1	**IA.L2-3.5.3** *Multifactor Authentication* Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. • NIST SP 800-171 Rev 2 3.5.3	
IA.L1-3.5.2 *Authentication* Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. • FAR Clause 52.204-21 b.1.vi • NIST SP 800-171 Rev 2 3.5.2	**IA.L2-3.5.4** *Replay-Resistant Authentication* Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts. • NIST SP 800-171 Rev 2 3.5.4	
	IA.L2-3.5.5 *Identifier Reuse* Prevent reuse of identifiers for a defined period. • NIST SP 800-171 Rev 2 3.5.5	
	IA.L2-3.5.6 *Identifier Handling* Disable identifiers after a defined period of inactivity. • NIST SP 800-171 Rev 2 3.5.6	
	IA.L2-3.5.7 *Password Complexity* Enforce a minimum password complexity and change of characters when new passwords are created. • NIST SP 800-171 Rev 2 3.5.7	
	IA.L2-3.5.8 *Password Reuse* Prohibit password reuse for a specified number of generations. • NIST SP 800-171 Rev 2 3.5.8	
	IA.L2-3.5.9 *Temporary Passwords* Allow temporary password use for system logons with an immediate change to a permanent password. • NIST SP 800-171 Rev 2 3.5.9	
	IA.L2-3.5.10 *Cryptographically-Protected Passwords* Store and transmit only cryptographically protected passwords. • NIST SP 800-171 Rev 2 3.5.10	
	IA.L2-3.5.11 *Obscure Feedback* Obscure feedback of authentication information. • NIST SP 800-171 Rev 2 3.5.11	

INCIDENT RESPONSE (IR)

Level 1	Level 2	Level 3 (TBD)
	IR.L2-3.6.1 *Incident Handling* Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. • NIST SP 800-171 Rev 2 3.6.1	
	IR.L2-3.6.2 *Incident Reporting* Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization. • NIST SP 800-171 Rev 2 3.6.2	
	IR.L2-3.6.3 *Incident Response Testing* Test the organizational incident response capability. • NIST SP 800-171 Rev 2 3.6.3	

MAINTENANCE (MA)

Level 1	Level 2	Level 3 (TBD)
	MA.L2-3.7.1 *Perform Maintenance* Perform maintenance on organizational systems. • NIST SP 800-171 Rev 2 3.7.1	
	MA.L2-3.7.2 *System Maintenance Control* Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. • NIST SP 800-171 Rev 2 3.7.2	
	MA.L2-3.7.3 *Equipment Sanitization* Ensure equipment removed for off-site maintenance is sanitized of any CUI. • NIST SP 800-171 Rev 2 3.7.3	
	MA.L2-3.7.4 *Media Inspection* Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. • NIST SP 800-171 Rev 2 3.7.4	
	MA.L2-3.7.5 *Nonlocal Maintenance* Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete. • NIST SP 800-171 Rev 2 3.7.5	
	MA.L2-3.7.6 *Maintenance Personnel* Supervise the maintenance activities of maintenance personnel without required access authorization. • NIST SP 800-171 Rev 2 3.7.6	

MEDIA PROECTION (MP)

Level 1	Level 2	Level 3 (TBD)
MP.L1-3.8.3 *Media Disposal* Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. • FAR Clause 52.204-21 b.1.vii • NIST SP 800-171 Rev 2 3.8.3	**MP.L2-3.8.1** *Media Protection* Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. • NIST SP 800-171 Rev 2 3.8.1	
	MP.L2-3.8.2 *Media Access* Limit access to CUI on system media to authorized users. • NIST SP 800-171 Rev 2 3.8.2	
	MP.L2-3.8.4 *Media Markings* Mark media with necessary CUI markings and distribution limitations. • NIST SP 800-171 Rev 2 3.8.4	
	MP.L2-3.8.5 *Media Accountability* Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. • NIST SP 800-171 Rev 2 3.8.5	
	MP.L2-3.8.6 *Portable Storage Encryption* Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards. • NIST SP 800-171 Rev 2 3.8.6	
	MP.L2-3.8.7 *Removable Media* Control the use of removable media on system components. • NIST SP 800-171 Rev 2 3.8.7	
	MP.L2-3.8.8 *Shared Media* Prohibit the use of portable storage devices when such devices have no identifiable owner. • NIST SP 800-171 Rev 2 3.8.8	
	MP.L2-3.8.9 *Protect Backups* Protect the confidentiality of backup CUI at storage locations. • NIST SP 800-171 Rev 2 3.8.9	

PERSONNEL SECURITY (PS)

Level 1	Level 2	Level 3 (TBD)
	PS.L2-3.9.1 *Screen Individuals* Screen individuals prior to authorizing access to organizational systems containing CUI. • NIST SP 800-171 Rev 2 3.9.1	
	PS.L2-3.9.2 *Personnel Actions* Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers. • NIST SP 800-171 Rev 2 3.9.2	

PHYSICAL PROTECTION (PE)

Level 1	Level 2	Level 3 (TBD)
PE.L1-3.10.1 *Limit Physical Access* Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. • FAR Clause 52.204-21 b.1.viii • NIST SP 800-171 Rev 2 3.10.1	**PE.L2-3.10.2** *Monitor Facility* Protect and monitor the physical facility and support infrastructure for organizational systems. • NIST SP 800-171 Rev 2 3.10.2	
PE.L1-3.10.3 *Escort Visitors* Escort visitors and monitor visitor activity. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.3	**PE.L2-3.10.6** *Alternative Work Sites* Enforce safeguarding measures for CUI at alternate work sites. • NIST SP 800-171 Rev 2 3.10.6	
PE.L1-3.10.4 *Physical Access Logs* Maintain audit logs of physical access. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.4		
PE.L1-3.10.5 *Manage Physical Access* Control and manage physical access devices. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.5		

RISK ASSESSMENT (RA)

Level 1	Level 2	Level 3 (TBD)
	RA.L2-3.11.1 *Risk Assessments* 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. • NIST SP 800-171 Rev 2 3.11.1	
	RA.L2-3.11.2 *Vulnerability Scan* Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. • NIST SP 800-171 Rev 2 3.11.2	
	RA.L2-3.11.3 *Vulnerability Remediation* Remediate vulnerabilities in accordance with risk assessments. • NIST SP 800-171 Rev 2 3.11.3	

SECURITY ASSESSMENT (CA)

Level 1	Level 2	Level 3 (TBD)
	CA.L2-3.12.1 *Security Control Assessment* Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. • NIST SP 800-171 Rev 2 3.12.1	
	CA.L2-3.12.2 *Plan of Action* Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. • NIST SP 800-171 Rev 2 3.12.2	
	CA.L2-3.12.3 *Security Control Monitoring* Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls. • NIST SP 800-171 Rev 2 3.12.3	
	CA.L2-3.12.4 *System Security Plan* 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. • NIST SP 800-171 Rev 2 3.12.4	

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Level 1	Level 2	Level 3 (TBD)
SC.L1-3.13.1 *Boundary Protection* 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. • FAR Clause 52.204-21 b.1.x • NIST SP 800-171 Rev 2 3.13.1	**SC.L2-3.13.2** *Security Engineering* Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems. • NIST SP 800-171 Rev 2 3.13.2	
SC.L1-3.13.5 *Public-Access System Separation* Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. • FAR Clause 52.204-21 b.1.xi • NIST SP 800-171 Rev 2 3.13.5	**SC.L2-3.13.3** *Role Separation* Separate user functionality from system management functionality. • NIST SP 800-171 Rev 2 3.13.3	
	SC.L2-3.13.4 *Shared Resource Control* Prevent unauthorized and unintended information transfer via shared system resources. • NIST SP 800-171 Rev 2 3.13.4	
	SC.L2-3.13.6 *Network Communication by Exception* Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). • NIST SP 800-171 Rev 2 3.13.6	
	SC.L2-3.13.7 *Split Tunneling* 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). • NIST SP 800-171 Rev 2 3.13.7	
	SC.L2-3.13.8 *Data in Transit* Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. • NIST SP 800-171 Rev 2 3.13.8	
	SC.L2-3.13.9 *Connections Termination* Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. • NIST SP 800-171 Rev 2 3.13.9	

Level 1	Level 2	Level 3 (TBD)
	SC.L2-3.13.10 *Key Management* Establish and manage cryptographic keys for cryptography employed in organizational systems. • NIST SP 800-171 Rev 2 3.13.10	
	SC.L2-3.13.11 *CUI Encryption* Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. • NIST SP 800-171 Rev 2 3.13.11	
	SC.L2-3.13.12 *Collaborative Device Control* Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. • NIST SP 800-171 Rev 2 3.13.12	
	SC.L2-3.13.13 *Mobile Code* Control and monitor the use of mobile code. • NIST SP 800-171 Rev 2 3.13.13	
	SC.L2-3.13.14 *Voice over Internet Protocol* Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. • NIST SP 800-171 Rev 2 3.13.14	
	SC.L2-3.13.15 *Communications Authenticity* Protect the authenticity of communications sessions. • NIST SP 800-171 Rev 2 3.13.15	
	SC.L2-3.13.16 *Data at Rest* Protect the confidentiality of CUI at rest. • NIST SP 800-171 Rev 2 3.13.16	

SYSTEM AND INFORMATION INTEGRITY (SI)

Level 1	Level 2	Level 3 (TBD)
SI.L1-3.14.1 *Flaw Remediation* Identify, report, and correct information and information system flaws in a timely manner. • FAR Clause 52.204-21 b.1.xii • NIST SP 800-171 Rev 2 3.14.1	**SI.L2-3.14.3** *Security Alerts & Advisories* Monitor system security alerts and advisories and take action in response. • NIST SP 800-171 Rev 2 3.14.3	
SI.L1-3.14.2 *Malicious Code Protection* Provide protection from malicious code at appropriate locations within organizational information systems. • FAR Clause 52.204-21 b.1.xiii • NIST SP 800-171 Rev 2 3.14.2	**SI.L2-3.14.6** *Monitor Communications for Attacks* Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks. • NIST SP 800-171 Rev 2 3.14.6	
SI.L1-3.14.4 *Update Malicious Code Protection* Update malicious code protection mechanisms when new releases are available. • FAR Clause 52.204-21 b.1.xiv • NIST SP 800-171 Rev 2 3.14.4	**SI.L2-3.14.7** *Identify Unauthorized Use* Identify unauthorized use of organizational systems. • NIST SP 800-171 Rev 2 3.14.7	
SI.L1-3.14.5 *System & File Scanning* Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. • FAR Clause 52.204-21 b.1.xv • NIST SP 800-171 Rev 2 3.14.5		

Appendix B. Source Mapping

This source mapping provides a detailed list of practices from other frameworks that are related to each CMMC practice. In this way, the mapping allows an organization to easily identify which CMMC practices correspond to sources in other frameworks that the organization may already be using or may need to reference in the future. These source mappings do not represent additional CMMC requirements.

The CMMC practices that align with the FAR Clause 52.204-21, NIST SP 800-171 Rev 2, and NIST SP 800-172 are identical to the reference practices. An organization that meets the requirements for the CMMC practice will also meet the requirements for these security requirements. The additional sources are for reference only and do not guarantee that if an organization meets the requirements of these secondary sources they will also meet the corresponding CMMC practice.

The following table summarizes related sources for each CMMC practice.

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 2	NIST SP 800-172	NIST SP 800-53 Rev 5	CIS Controls v7.1	NIST CSF v1.1	CERT-RMM v1.2	Other
Access Control (AC)	AC.L1-3.1.1	b.1.i	3.1.1		AC-2, AC-3, AC-17	1.4, 1.6, 14.6	PR.AC-3, PR.AC-4, PR.PT-3	TM:SG4:SP1, AM.SG1	
	AC.L1-3.1.2	b.1.ii	3.1.2		AC-2, AC-3, AC-17		PR.AC-3, PR.AC-4, PR.PT-3	TM:SG4:SP1, AM.SG1.SP1	
	AC.L1-3.1.20	b.1.iii	3.1.20		AC-20, AC-20(1)		ID.AM-4, PR.AC-3		
	AC.L1-3.1.22	b.1.iv	3.1.22		AC-22				
	AC.L2-3.1.3		3.1.3		AC-4	12.1, 12.2, 12.5, 13.3, 14.1, 14.6	ID.AM-3, PR.AC-5	TM:SG4:SP1	
	AC.L2-3.1.4		3.1.4		AC-5		PR.AC-4, PR.DS-5		
	AC.L2-3.1.5		3.1.5		AC-6, AC-6(1), AC-6(5)	14.6	PR.AC-4	AM.SG1.SP1, AM.SG1.SP3	UK NCSC Cyber Essentials
	AC.L2-3.1.6		3.1.6		AC-6(2)	4.3, 4.6	PR.AC-4	AM.SG1.SP1	UK NCSC Cyber Essentials
	AC.L2-3.1.7		3.1.7		AC-6(9), AC-6(10)	4.1	PR.AC-4	KIM:SG4:SP1, AM.SG1.SP4	
	AC.L2-3.1.8		3.1.8		AC-7		PR.AC-4		UK NCSC Cyber Essentials
	AC.L2-3.1.9		3.1.9		AC-8				
	AC.L2-3.1.10		3.1.10		AC-11, AC-11(1)	16.11	PR.AC-4		
	AC.L2-3.1.11		3.1.11		AC-12	16.11	PR.AC-4		
	AC.L2-3.1.12		3.1.12		AC-17(1)	12.11, 12.12	DE.CM-3, DE.CM-7	TM:SG2:SP2	
	AC.L2-3.1.13		3.1.13		AC-17(2)	15.7, 15.8	PR.DS-2, PR.DS-5	KIM:SG4:SP1	
	AC.L2-3.1.14		3.1.14		AC-17(3)	15.5, 15.10	PR.AC-3	TM:SG2:SP2	
	AC.L2-3.1.15		3.1.15		AC-17(4)	8.8, 12.11, 12.12	PR.AC-3	TM:SG2:SP2	
	AC.L2-3.1.16		3.1.16		AC-18	15.1, 15.10	PR.PT-4	TM:SG2:SP2	
	AC.L2-3.1.17		3.1.17		AC-18(1)	15.7, 15.8	PR.DS-2, PR.PT-4	KIM:SG4:SP1	
	AC.L2-3.1.18		3.1.18		AC-19	13.6	PR.AC-3	TM:SG2	
	AC.L2-3.1.19		3.1.19		AC-19(5)	13.6	PR.DS-1	KIM:SG4:SP1	
	AC.L2-3.1.21		3.1.21		AC-20(2)	13.7, 13.8, 13.9	ID.AM-4		

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 2	NIST SP 800-172	NIST SP 800-53 Rev 5	CIS Controls v7.1	NIST CSF v1.1	CERT-RMM v1.2	Other
Awareness and Training (AT)	AT.L2-3.2.1		3.2.1		AT-2, AT-3	17.3	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5	OTA:SG1.SP1, OTA:SG2.SP1	
	AT.L2-3.2.2		3.2.2		AT-2, AT-3	17.1, 17.2 17.5, 17.6, 17.7, 17.8, 17.9	PR.AT-1, PR.AT-2, PR.AT-4, PR.AT-5	OTA:SG4.SP1	
	AT.L2-3.2.3		3.2.3		AT-2(2)		PR.AT-1, PR.DS-5	OTA:SG1.SP1, OTA:SG2:SP1	
Audit and Accountability (AU)	AU.L2-3.3.1		3.3.1		AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	6.2	PR.PT-1, DE.AE-2, DE.CM-3, DE.CM-7	MON:SG2.SP3	
	AU.L2-3.3.2		3.3.2		AU-2, AU-3, AU-3(1), AU-6, AU-11, AU-12	16.8, 16.9	PR.PT-1, DE.AE-2, DE.CM-3	MON:SG1.SP3, MON:SG2.SP3	
	AU.L2-3.3.3		3.3.3		AU-2	6.7	PR.PT-1	IMC:SG2:SP2	
	AU.L2-3.3.4		3.3.4		AU-5	6.7	PR.PT-1	MON:GG2.GP8	
	AU.L2-3.3.5		3.3.5		AU-6(3)	6.6, 6.7	PR.PT-1, DE.AE-2, DE.AE-3, RS.AN-1	COMP: SG3:SP1	
	AU.L2-3.3.6		3.3.6		AU-7	6.6	PR.PT-1		
	AU.L2-3.3.7		3.3.7		AU-8, SC-45(1)	6.1	PR.PT-1		
	AU.L2-3.3.8		3.3.8		AU-9		PR.PT-1	MON:SG2.SP3	
	AU.L2-3.3.9		3.3.9		AU-9(4)		PR.PT-1	MON:SG2.SP2	
Configuration Management (CM)	CM.L2-3.4.1		3.4.1		CM-2, CM-6, CM-8, CM-8(1)	1.4, 1.5, 2.1, 2.4, 5.1, 5.2	ID.AM-1, ID.AM-2, PR.DS-3, PR.IP-1	KIM:SG5.SP2	UK NCSC Cyber Essentials
	CM.L2-3.4.2		3.4.2		CM-2, CM-6, CM-8, CM-8(1)	1.4, 1.5, 2.1, 2.4, 5.1	PR.IP-1	TM:SG2:SP2	UK NCSC Cyber Essentials
	CM.L2-3.4.3		3.4.3		CM-3	6.3	PR.IP-3	KIM:SG5.SP2	
	CM.L2-3.4.4		3.4.4		CM-4		PR.IP-3	TM:SG4.SP3	
	CM.L2-3.4.5		3.4.5		CM-5	2.5, 2.7, 2.8, 2.9, 4.3, 4.6	PR.IP-3	TM:SG4:SP1	UK NCSC Cyber Essentials
	CM.L2-3.4.6		3.4.6		CM-7	9.2	PR.IP-1, PR.PT-3	TM:SG2:SP2	UK NCSC Cyber Essentials
	CM.L2-3.4.7		3.4.7		CM-7(1), CM-7(2)	9.2, 9.4, 12.4	PR.IP-1, PR.PT-3		UK NCSC Cyber Essentials
	CM.L2-3.4.8		3.4.8		CM-7(4), CM-7(5)	2.7, 2.8, 2.9	PR.IP-1, PR.PT-3	TM:SG2:SP2	UK NCSC Cyber Essentials; AU ACSC Essential Eight
	CM.L2-3.4.9		3.4.9		CM-11	2.1, 2.2, 2.6	DE.CM-3	MON:SG2:SP3	

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 2	NIST SP 800-172	NIST SP 800-53 Rev 5	CIS Controls v7.1	NIST CSF v1.1	CERT-RMM v1.2	Other
Identification and Authentication (IA)	IA.L1-3.5.1	b.1.v	3.5.1		IA-2, IA-3, IA-5	4.3, 16.6	PR.AC-1	ID:SG1:SP1	
	IA.L1-3.5.2	b.1.vi	3.5.2		IA-2, IA-3, IA-5	4.2, 16.8	PR.AC-1	TM:SG4:SP1	UK NCSC Cyber Essentials
	IA.L2-3.5.3		3.5.3		IA-2(1), IA-2(2)	4.5, 11.5, 12.11	PR.AC-4	TM:SG4:SP1	UK NCSC Cyber Essentials; AU ACSC Essential Eight
	IA.L2-3.5.4		3.5.4		IA-2(8)		PR.AC-4		
	IA.L2-3.5.5		3.5.5		IA-4	16.7, 16.10, 16.12	PR.AC-1	ID:SG2.SP4	
	IA.L2-3.5.6		3.5.6		IA-4	16.9, 16.10, 16.11	PR.AC-1	ID:SG2.SP4	UK NCSC Cyber Essentials
	IA.L2-3.5.7		3.5.7		IA-5(1)	4.2, 4.4	PR.AC-1		UK NCSC Cyber Essentials
	IA.L2-3.5.8		3.5.8		IA-5(1)	4.2, 4.4	PR.AC-1		
	IA.L2-3.5.9		3.5.9		IA-5(1)		PR.AC-1		
	IA.L2-3.5.10		3.5.10		IA-5(1)	16.4, 16.5	PR.AC-1	KIM:SG4:SP1	
	IA.L2-3.5.11		3.5.11		IA-6		PR.AC-1		
Incident Response (IR)	IR.L2-3.6.1		3.6.1		IR-2, IR-4, IR-5, IR-6, IR-7	19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.8	PR.IP-9 DE.AE-2 DE.AE-5 RS.CO-4 RS.AN-1 RS.AN-4 RS.MI-1 RS.MI-2 RS.IM-1 RC.RP-1 RC.IM-1 RC.IM-2 RC.CO-3	IMC:SG1:SP1	
	IR.L2-3.6.2		3.6.2		IR-2, IR-4, IR-5, IR-6, IR-7	19.4	PR.IP-9 DE.AE-5 RS.RP-1 RS.CO-2 RS.AN-1 RS.AN-4 RS.MI-1 RS.MI-2 RS.IM-1 RS.IM-2 RC.RP-1 RC.IM-1 RC.IM-2 RC.CO-3	IMC:SG2:SP2	
	IR.L2-3.6.3		3.6.3		IR-3	19.7	PR.IP-10 RS.CO-1		

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 2	NIST SP 800-172	NIST SP 800-53 Rev 5	CIS Controls v7.1	NIST CSF v1.1	CERT-RMM v1.2	Other
Maintenance (MA)	MA.L2-3.7.1		3.7.1		MA-2, MA-3, MA-3(1), MA-3(2)	3.4, 3.5	PR.MA-1	TM:SG5.SP2	
	MA.L2-3.7.2		3.7.2		MA-2, MA-3, MA-3(1), MA-3(2)		PR.MA-1	TM:SG5:SP2	
	MA.L2-3.7.3		3.7.3		MA-2		PR.MA-1	TM:SG5:SP2	
	MA.L2-3.7.4		3.7.4		MA-3(2)		PR.MA-1		
	MA.L2-3.7.5		3.7.5		MA-4		PR.MA-2	TM:SG4:SP1	
	MA.L2-3.7.6		3.7.6		MA-5		PR.MA-1	TM:SG5:SP2, TM:SG4.SP1	
Media Protection (MP)	MP.L1-3.8.3	b.1.vii	3.8.3		MP-2, MP-4, MP-6		PR.DS-3 PR.IP-6 PR.PT-2	KIM:SG4:SP3	
	MP.L2-3.8.1		3.8.1		MP-2, MP-4, MP-6		PR.DS-1 PR.DS-3 PR.PT-2	KIM:SG2.SP2	
	MP.L2-3.8.2		3.8.2		MP-2, MP-4, MP-6	14.6	PR.DS-3 PR.PT-2	MON:SG2.SP4	
	MP.L2-3.8.4		3.8.4		MP-3		PR.PT-2	MON:SG2.SP4	
	MP.L2-3.8.5		3.8.5		MP-5		PR.DS-2 PR.DS-3 PR.PT-2	KIM:SG4:SP2	
	MP.L2-3.8.6		3.8.6		SC-28(1)	13.9	PR.PT-2	KIM:SG4:SP1	
	MP.L2-3.8.7		3.8.7		MP-7	13.7, 13.8	PR.PT-2	MON:SG2.SP4	
	MP.L2-3.8.8		3.8.8		MP-7	13.7	PR.PT-2	MON:SG2.SP4	
	MP.L2-3.8.9		3.8.9		CP-9	10.4	PR.DS-1	AM:SG1.SP1	
Personnel Security (PS)	PS.L2-3.9.1		3.9.1		PS-3, PS-4, PS-5		PR.IP-11	HRM:SG2.SP1	
	PS.L2-3.9.2		3.9.2		PS-3, PS-4, PS-5	16.7	PR.DS-5 PR.IP-11	HRM:SG4.SP2	
Physical Protection (PE)	PE.L1-3.10.1	b.1.viii	3.10.1		PE-2, PE-4, PE-5, PE-6		PR.AC-2	KIM:SG4.SP2	
	PE.L1-3.10.3	b.1.ix	3.10.3		PE-3		PR.AC-2 DE.CM-2 DE.CM-7	AM:SG1:SP1	
	PE.L1-3.10.4	b.1.ix	3.10.4		PE-3		PR.AC-2 DE.DP-3	MON:SG2.SP3	
	PE.L1-3.10.5	b.1.ix	3.10.5		PE-3		PR.AC-2	KIM:SG4.SP2	
	PE.L2-3.10.2		3.10.2		PE-2, PE-4, PE-5, PE-6		PR.AC-2 DE.CM-2 DE.CM-7	KIM:SG4.SP2	
	PE.L2-3.10.6		3.10.6		PE-17			EC:SG2:SP1	

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 2	NIST SP 800-172	NIST SP 800-53 Rev 5	CIS Controls v7.1	NIST CSF v1.1	CERT-RMM v1.2	Other
Risk Assessment (RA)	RA.L2-3.11.1		3.11.1		RA-3		ID.RA-1 ID.RA-3 ID.RA-4 ID.RA-5 DE.AE-4 RS.AN-2 RS.MI-3	RISK:SG4	
	RA.L2-3.11.2		3.11.2		RA-5, RA-5(5)	3.1, 3.2	ID.RA-1 PR.IP-12 DE.CM-8 RS.MI-3	VAR:SG2:SP2	
	RA.L2-3.11.3		3.11.3		RA-5	3.7	RS.MI-3	VAR:SG3.SP1	
Security Assessment (CA)	CA.L2-3.12.1		3.12.1		CA-2, CA-5, CA-7, PL-2		ID.RA-1 DE.DP-2 DE.DP-3		
	CA.L2-3.12.2		3.12.2		CA-2, CA-5, CA-7, PL-2		PR.IP-12 RS.MI-3	RISK:SG5:SP1	
	CA.L2-3.12.3		3.12.3		CA-2, CA-5, CA-7, PL-2		ID.RA-1 PR.IP-12 DE.DP-2 DE.DP-3	MON:SG1:SP1	
	CA.L2-3.12.4		3.12.4		CA-2, CA-5, CA-7, PL-2		RS.MI-3		
System and Communications Protection (SC)	SC.L1-3.13.1	b.1.x	3.13.1		SC-7, SC-8	12.5, 12.9	ID.AM-3 PR.AC-5 PR.DS-5 PR.PT-4 DE.CM-1		UK NCSC Cyber Essentials
	SC.L1-3.13.5	b.1.xi	3.13.5		SC-7	14.1	PR.AC-5 PR.DS-5 PR.PT-4		UK NCSC Cyber Essentials
	SC.L2-3.13.2		3.13.2		SC-7, SC-8	5.1, 5.2, 5.4	PR.AC-5 PR.PT-4		
	SC.L2-3.13.3		3.13.3		SC-2	4.3	PR.AC-4	KIM:SG2:SP2	AU ACSC Essential Eight
	SC.L2-3.13.4		3.13.4		SC-4		PR.AC-4		
	SC.L2-3.13.6		3.13.6		SC-7(5)	13.3	PR.AC-5 PR.DS-5 PR.PT-4		
	SC.L2-3.13.7		3.13.7		SC-7(7)	12.12	PR.AC-5 PR.DS-5 PR.PT-4		
	SC.L2-3.13.8		3.13.8		SC-8, SC-8(1)	14.4	PR.DS-2 PR.DS-5	KIM:SG4:SP1	
	SC.L2-3.13.9		3.13.9		SC-10		PR.AC-3		
	SC.L2-3.13.10		3.13.10		SC-12		PR.DS-1 PR.DS-2	KIM:SG4:SP1	
	SC.L2-3.13.11		3.13.11		SC-13	14.4, 14.8	PR.DS-5	KIM:SG4:SP1	
	SC.L2-3.13.12		3.13.12		SC-15		PR.AC-3		
	SC.L2-3.13.13		3.13.13		SC-18	7.3	DE.CM-5		AU ACSC Essential Eight
	SC.L2-3.13.14		3.13.14		AU-6				
	SC.L2-3.13.15		3.13.15		SC-23		PR.PT-4		
	SC.L2-3.13.16		3.13.16		SC-28	14.8	PR.DS-1 PR.DS-5		

Domain	CMMC Practice ID	FAR Clause 52.204-21	NIST SP 800-171 Rev 2	NIST SP 800-172	NIST SP 800-53 Rev 5	CIS Controls v7.1	NIST CSF v1.1	CERT-RMM v1.2	Other
System and Information Integrity (SI)	SI.L1-3.14.1	b.1.xii	3.14.1		SI-2, SI-3, SI-5		ID.RA-1 ID.RA-2 ID.RA-3 PR.IP-12 DE.CM-4 RS.MI-3	VAR:SG2:SP2	UK NCSC Cyber Essentials; AU ACSC Essential Eight
	SI.L1-3.14.2	b.1.xiii	3.14.2		SI-2, SI-3, SI-5	8.1	PR.IP-12 DE.CM-4	VAR:SG3:SP1	UK NCSC Cyber Essentials; AU ACSC Essential Eight
	SI.L1-3.14.4	b.1.xiv	3.14.4		SI-3	8.2	DE.CM-4	VAR:SG3:SP1	UK NCSC Cyber Essentials
	SI.L1-3.14.5	b.1.xv	3.14.5		SI-3	8.4	DE.CM-4	VAR:SG3:SP1	UK NCSC Cyber Essentials
	SI.L2-3.14.3		3.14.3		SI-2, SI-3, SI-5		ID.RA-1 ID.RA-2 ID.RA-3 PR.IP-12 DE.CM-4	IMC:SG2:SP1	
	SI.L2-3.14.6		3.14.6		SI-4, SI-4(4)	12.6	ID.RA-1 PR.DS-5 DE.AE-2 DE.CM-1 DE.CM-6 DE.CM-7 DE.DP-2	MON:SG1:SP3	
	SI.L2-3.14.7		3.14.7		SI-4	6.7, 12.2	ID.RA-1 DE.AE-2 DE.CM-1 DE.CM-6 DE.CM-7 DE.DP-2	MON:SG1:SP3	

Appendix C. Abbreviations and Acronyms

The following is a list of acronyms used in the CMMC model.

AC	Access Control
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
AIA	Aerospace Industries Association
APT	Advanced Persistent Threat
AT	Awareness and Training
AU	Audit and Accountability
BYOD	Bring Your Own Device
C2M2	Cybersecurity Capability Maturity Model
CA	Security Assessment
CEA	Council of Economic Advisers
CERT	Computer Emergency Response Team
CERT RMM	CERT® Resilience Management Model
CFR	Code of Federal Regulations
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instructions
COMSEC	Communications Security
CPI	Critical Program Information
CSF	Cybersecurity Framework
CSIS	Center for Strategic and International Studies
CSP	Credential Service Provider
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DNS	Domain Name System
DoD	Department of Defense
DoDI	DoD Instruction
DPCI	Derived PIV Credential Issuers
E.O.	Executive Order

FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
ICS	Industrial Control System
IDPS	Intrusion Detection and Prevention Systems
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IR	Incident Response
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISO	International Organization for Standardization
ISCM	Information Security Continuous Monitoring
ITIL	Information Technology Infrastructure Library
L#	Level Number
MA	Maintenance
MP	Media Protection
N/A	Not Applicable (NA)
NAS	National Aerospace Standard
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency (or Internal) Report
NSA	National Security Agency
NSA/CSS	NSA Central Security Service
NSPD	National Security Presidential Directive
NYSSCPA	New York State Society of CPAs
OMB	Office of Management and Budget
OS	Operating System
OUSD A&S	Office of the Under Secretary of Defense for Acquisition and Sustainment
PCI	Personal Identity Verification Card Issuers
PE	Physical Protection
PIV	Personal Identity Verification
PKI	Public Key Infrastructure

PPD	Presidential Policy Directive
PS	Personnel Security
PUB	Publication
Rev	Revision
RFC	Request for Comments
RA	Risk Asssessment
RMM	Risk Management Model
SC	System and Communications Protection
SCRM	Supply Chain Risk Management
SI	System and Information Integrity
SP	Special Publication
SSP	Sector Specific Plan
TTP	Tactics, Techniques, and Procedures
UARC	University Affiliated Research Center
UK	United Kingdom
URL	Uniform Resource Locator
U.S.	United States
VoIP	Voice over Internet Protocol
Vol.	Volume

Appendix D. References

1. U.S. Executive Office of the President, Council of Economic Advisers (CEA). *The Cost of Malicious Cyber Activity to the U.S. Economy*, available online at https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf, February 2018

2. Center for Strategic and International Studies (CSIS) and McAfee, *Economic Impact of Cybercrime - No Slowing Down*, February 2018

3. 48 Code of Federal Regulations (CFR) 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, Federal Acquisition Regulation (FAR), 1 Oct 2016

4. NIST Special Publication (SP) 800-171 Revision (Rev) 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, U.S. Department of Commerce National Institute of Standards and Technology (NIST), December 2016 (updated June 2018)

5. DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, October 2016

6. NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, U.S. Department of Commerce National Institute of Standards and Technology (NIST), February 2021

7. United Kingdom (UK) Cyber Essentials, National Cyber Security Centre (NCSC), available online https://www.cyberessentials.ncsc.gov.uk

8. *Essential Eight Maturity Model*, Australian Cyber Security Centre (ACSC), July 2018

9. *Cybersecurity Capability Maturity Model (C2M2)*, Version 1.1, Department of Energy, Department of Homeland Security, and Carnegie Mellon University Software Engineering Institute, February 2017

10. *Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale*, Technical Note CMU/SEI-2013-TN-028, M. J. Butkovic and R. A. Caralli, Carnegie Mellon University Software Engineering Institute, November 2013

11. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011

12. FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, Department of Commerce, March 2006

13. CERT® Resilience Management Model (CERT RMM) Version 1.2, *A Maturity Model for Managing Operational Resilience*, Carnegie Mellon University Software Engineering Institute, February 2016

14. FIPS PUB 197, *Advanced Encryption Standard (AES)*, November 2001

15. FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

16. FIPS PUB 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors,* August 2013

17. National Aerospace Standard (NAS) NAS9933, *Critical Security Controls for Effective Capability in Cyber Defense*, Aerospace Industries Association (AIA), 2018

18. NIST Cybersecurity Framework (CSF), *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018

19. NIST SP 800-114 Rev. 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, July 2016

20. NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008

21. NIST SP 800-12 Rev. 1, *An Introduction to Information Security*, June 2017

22. NIST SP 800-123, *Guide to General Server Security*, July 2008

23. NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011 (Updated October 2019)

24. NIST SP 800-150, *Guide to Cyber Threat Information Sharing*, October 2016

25. NIST SP 800-16, *Information Technology Security Training Requirements: a Role- and Performance-Based Model*, April 1998

26. NIST SP 800-160 Vol. 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, November 2016 (Updated March 2018)

27. NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015

28. NIST SP 800-171 Rev. 1, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, December 2016

29. NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
30. NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, September 2012
31. NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001
32. NIST SP 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*, May 2010 (updated November 2010)
33. NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018
34. NIST SP 800-41 Rev 2, *Guidelines on Firewalls and Firewall Policy*, September 2009
35. NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (updated January 2015)
36. NIST SP 800-57 Part 1 Rev. 4, *Recommendation for Key Management*, January 2016
37. NIST SP 800-57 Part 2 Rev. 1, *Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations*, May 2019
38. NIST SP 800-61, *Computer Security Incident Handling Guide*, August 2012
39. NIST SP 800-63-3, *Digital Identity Guidelines*, June 2017
40. NIST SP 800-66 Rev. 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008
41. NIST SP 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006
42. NIST SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015
43. NIST SP 800-82 Rev. 2, *Guide to Industrial Control Systems (ICS) Security*, May 2015
44. NIST SP 800-83 Rev. 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013
45. NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
46. NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2016

47. NIST SP 800-88 Rev. 1, *Guidelines for Media Sanitization*, December 2014

48. NIST SP 800-92, *Guide to Computer Security Log Management*, September 2006

49. NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007

50. NIST SP 800-95, *Guide to Secure Web Services*, August 2007

51. Center for Internet Security (CIS) Critical Security Controls version 7.1, available online at https://www.cisecurity.org/controls/, July 2019

52. ISO/IEC 27001:2013, *International Organization for Standardization (ISO): Information Security Management,* available online at: https://www.iso.org/isoiec-27001-information-security.html, 2019

53. National Institute of Standards and Technology Interagency or Internal Report (NISTIR) 7298 Rev. 3, *Glossary of Key Information Security Terms*, July 2019

54. NISTIR 7298 Rev. 3, *Glossary of Key Information Security Terms*, July 2019

55. NISTIR 7316, *Assessment of Access Control Systems*, September 2006

56. NISTIR 7621 Rev. 1, *Small Business Information Security: The Fundamentals*, November 2016

57. NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012

58. NISTIR 8053, *De-Identification of Personal Information*, October 2015

59. NISTIR 8074 Vol. 2, *Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, December 2015

60. NISTIR 8149, *Develop Trust Frameworks to Support Identity Federations*, January 2018

61. Committee on National Security Systems Directive (CNSSD) 504, *Directive on Protecting National Security Systems from Insider Threat*, September 2016

62. CNSSD 505, *Supply Chain Risk Management (SCRM)*, August 2017

63. Committee on National Security Systems Instruction (CNSSI) 4009, *Committee on National Security Systems Glossary*, April 2015

64. CNSSI 1011, *Implementing Host-Based Security Capabilities on National Security Systems*, July 2013

65. CNSSI 4005, *Safeguarding COMSEC Facilities and Materials*, August 2011

66. Oxford Dictionary, *Oxford Dictionary of English 3rd Edition,* 2015

67. Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience*, February 2013

68. Office of Management and Budget (OMB) M-17-09, *Management of Federal High Value Assets*, December 2016

69. New York State Society of CPAs (NYSSCPA), *Accounting Terminology Guide*, 2019

70. National Security Presidential Directive (NSPD) 54, *Cybersecurity Policy*, January 2008

71. Homeland Security Presidential Directive (HSPD) 23, *Cybersecurity Policy*, January 2008

72. NSA Central Security Service (NSA/CSS) Policy Manual 3-16, *Control of Communications Security (COMSEC)*, August 2005

73. Internet Engineering Task Force (IETF) Request for Comments (RFC) 4949 Version 2, *Internet Security Glossary*, August 2007

74. DHS Cybersecurity and Infrastructure Security Agency (CISA) Sector Specific Plan (SSP), *Defense Industrial Base (DIB) Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan,* May 2007

75. DHS Baseline Risk Assessment, *Information Technology Sector Baseline Risk Assessment*, August 2009

76. Executive Order (E.O.) 13556, *Controlled Unclassified Information*, November 2010

77. DoD Instruction (DoDI) 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense*, July 2018

78. DoDI 5000.02, *Operation of the Defense Acquisition System*, January 2015

79. 44 U.S. Code Section 3542, *Public Printing and Documents: Definitions*, January 2012

80. European Union General Data Protection Regulation (GDPR), online at https://eugdpr.org/


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