Cybersecurity Maturity Model Certification (CMMC) Model Overview

Version 2.13 | September 2024

DoD-CIO-00001 (ZRIN 0790-ZA17)

24-T-2765

NOTICES

The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide clarity to the public regarding existing CMMC security requirements under the law or departmental policies.

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

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]. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs.

Malicious cyber actors have targeted and continue to target the Defense Industrial Base (DIB) sector and the Department of Defense (DoD) supply chain. These attacks not only focus on the large prime contractors, but also target subcontractors that make up the lower tiers of the DoD supply chain. Many of these subcontractors are small entities that provide critical support and innovation. Overall, the DIB sector consists of over 220,000 companies[1] that process, store, or transmit Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) in support of 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 controlled unclassified information from the DoD supply chain can undercut U.S. technical advantages and innovation, as well as significantly increase the 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 enforce the safeguarding requirements of the following types of unclassified information within the supply chain:

- *Federal Contract Information (FCI*): is defined in 32 CFR § 170.4 and 48 CFR 4.1901 [3].
- *Controlled Unclassified Information (CUI):* is defined in 32 CFR § 2002.4 (h) [4].

To this end, the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) and DoD Chief Information Officer (CIO) have developed the Cybersecurity Maturity Model Certification (CMMC) 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 Cybersecurity Maturity Model Certification (CMMC) Model as set forth in section 170.14 of title 32, Code of Federal Regulations (CFR). The model

[1] Based on information from the Federal Procurement Data System, the average number of unique prime contractors is approximately 212,657 and the number of known unique subcontractors is approximately 8,309. (FPDS from FY18-FY21).

incorporates the security requirements from: 1) FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, 2) NIST SP 800-171 Rev 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and 3) 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 CMMC Program is designed to provide increased assurance to the DoD that defense contractors and subcontractors are compliant with information protection requirements for FCI and CUI, and are protecting such information at a level commensurate with risk from cybersecurity threats, including Advanced Persistent Threats (APTs).

When implementing the CMMC model, an organization can achieve a specific CMMC level for its entire enterprise network or for a particular 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 and maps the CMMC model to other secondary sources. Appendix B lists the abbreviations and acronyms. Finally, Appendix C provides the references contained in this document.

1.2 Supporting Documents

This document is supported by multiple companion documents that provide additional information. The *CMMC Assessment Guides* present assessment objectives, discussion, examples, potential assessment considerations, and key references for each CMMC security requirement. The *CMMC Scoping Guides* provide additional guidance on how to correctly scope an assessment. The *CMMC Hashing Guide* provides information on how to create the hash to validate the integrity of archived assessment artifacts.

These supplemental documents are intended to provide explanatory information to assist organizations with implementing and assessing the security requirements covered by CMMC in 32 CFR § 170. The documents are not prescriptive and their use is optional. Implementation of security requirements by following any examples is not a guarantee of compliance with any CMMC security requirement or objective.

2. CMMC Model

2.1 Overview

The CMMC Model incorporates the security requirements from: 1) FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*, 2) NIST SP 800-171 Rev 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, and 3) 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.* These source documents may be revised in the future, however the CMMC security requirements will remain unchanged until the CMMC final rule is published. Any further modifications to the CMMC rule will follow appropriate rulemaking procedures.

The CMMC Model consists of domains that map to the Security Requirement Families defined in NIST SP 800-171 Rev 2.

2.2 CMMC Levels

There are three levels within CMMC – Level 1, Level 2, and Level 3.

2.2.1 Descriptions

The CMMC model measures the implementation of cybersecurity requirements at three levels. Each level is independent and consists of a set of CMMC security requirements as set forth in 32 CFR § 170.14 (c):

- Level 1 Requirements. The security requirements in Level 1 are those set forth in FAR clause 52.204-21(b)(1)(i) – (b)(1)(xv).
- Level 2 Requirements. The security requirements in Level 2 are identical to the requirements in NIST SP 800-171 Rev 2.
- Level 3 Requirements. The security requirements in Level 3 are derived from NIST SP 800-172 with DoD-approved parameters where applicable, as identified in 32 CFR § 170.14(c)(4). DoD defined selections and parameters for the NIST SP 800-172 requirements are italicized, where applicable.

2.2.2 CMMC Overview

Figure 1 provides an overview of the CMMC Levels.

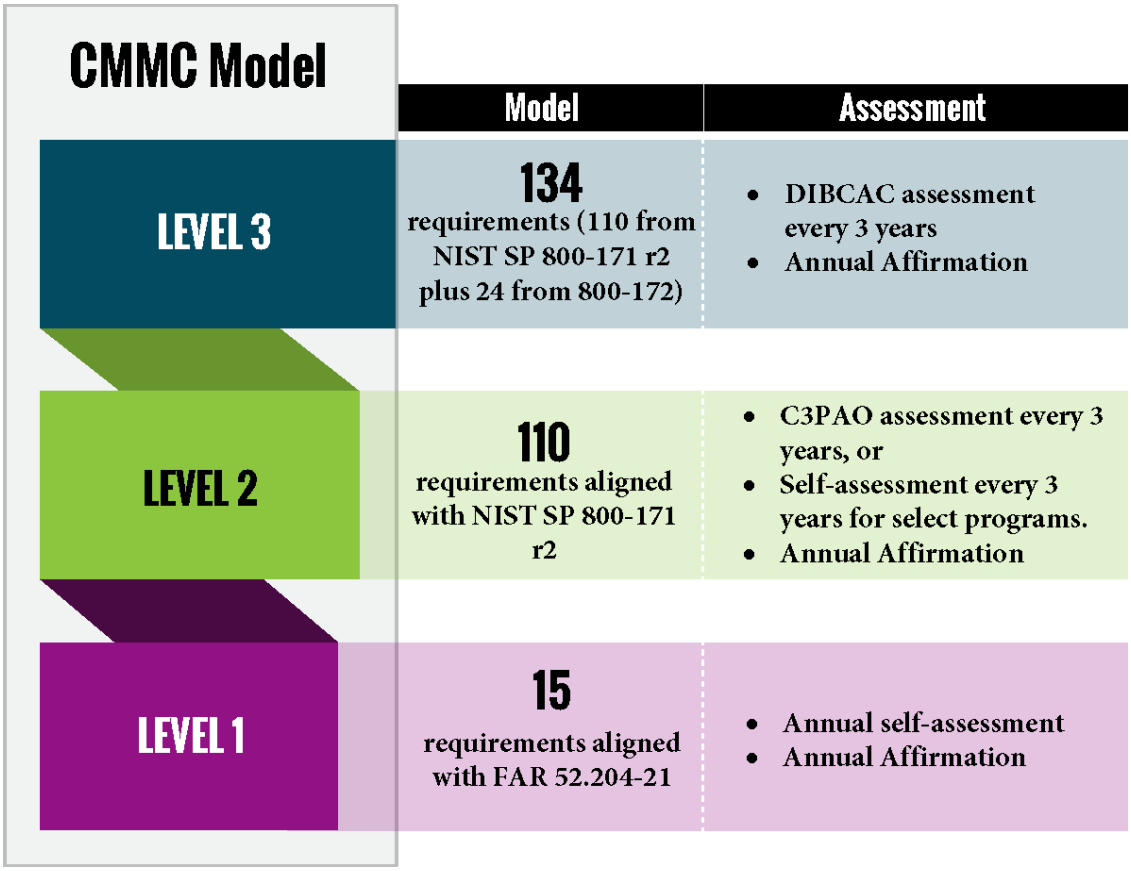

Figure 1. CMMC Level Overview

2.2.3 Level 1

Level 1 focuses on the protection of FCI and consists of the security requirements that correspond to the 15 basic safeguarding requirements specified in 48 CFR 52.204-21, commonly referred to as the FAR Clause.

2.2.4 Level 2

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

2.2.5. Level 3

Level 3 focuses on the protection of CUI and encompasses a subset of the NIST SP 800-172 security requirements [5] with DoD-approved parameters. DoD-approved parameters are denoted with underlining in section 2.4.1 below.

2.3 CMMC Domains

The CMMC model consists of 14 domains that align with the families specified in NIST SP 800-171 Rev 2. 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 Security Requirements

2.4.1. List of Security Requirements

This subsection itemizes the security requirements for each domain and at each level. Each requirement has a requirement 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 FAR Clause 52.204-21 paragraph number, 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 requirement, meant to be used for quick reference only. Finally, each requirement has a complete requirement statement.

ACCESS CONTROL (AC)

Level 1	Description
AC.L1-b.1.i *Authorized Access Control [FCI Data]*	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
AC.L1-b.1.ii *Transaction & Function Control [FCI Data]*	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
AC.L1-b.1.iii *External Connections [FCI Data]*	Verify and control/limit connections to and use of external information systems.
AC.L1-b.1.iv *Control Public Information [FCI Data]*	Control information posted or processed on publicly accessible information systems.

Level 2	Description
AC.L2-3.1.1 *Authorized Access Control [CUI Data]*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
AC.L2-3.1.2 *Transaction & Function Control [CUI Data]*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.
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.L2-3.1.20 *External Connections [CUI Data]*	Verify and control/limit connections to and use of external systems.
AC.L2-3.1.21 *Portable Storage Use*	Limit use of portable storage devices on external systems.
AC.L2-3.1.22 *Control Public Information [CUI Data]*	Control CUI posted or processed on publicly accessible systems.

Level 3	Description
AC.L3-3.1.2e *Organizationally Controlled Assets*	Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization.
AC.L3-3.1.3e *Secured Information Transfer*	Employ secure information transfer solutions to control information flows between security domains on connected systems.

AWARENESS AND TRAINING (AT)

Level 2	Description
AT.L2-3.2.1 *Role-Based Risk Awareness*	Inform managers, systems administrators, and users of organizational systems 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*	Train personnel 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	Description
AT.L3-3.2.1e *Advanced Threat Awareness*	Provide awareness training upon initial hire, following a significant cyber event, and at least annually, 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.L3-3.2.2e *Practical Training Exercises*	Include practical exercises in awareness training for all users, tailored by roles, to include general users, users with specialized roles, and privileged users, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.

AUDIT AND ACCOUNTABILITY (AU)

Level 2	Description
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*	Uniquely trace the actions of individual system 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.

CONFIGURATION MANAGEMENT (CM)

Level 2	Description
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	Description
CM.L3-3.4.1e *Authoritative Repository*	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.
CM.L3-3.4.2e *Automated Detection & Remediation*	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place the components in a quarantine or remediation network to facilitate patching, re-configuration, or other mitigations.
CM.L3-3.4.3e *Automated Inventory*	Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components.

IDENTIFICATION AND AUTHENTICATION (IA)

Level 1	Description
IA.L1-b.1.v *Identification [FCI Data]*	Identify information system users, processes acting on behalf of users, or devices.
IA.L1-b.1.vi *Authentication [FCI Data]*	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Level 2	Description
IA.L2-3.5.1 *Identification [CUI Data]*	Identify system users, processes acting on behalf of users, and devices.
IA.L2-3.5.2 *Authentication [CUI Data]*	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.
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	Description
IA.L3-3.5.1e *Bidirectional Authentication*	Identify and authenticate systems and system components, where possible, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.
IA.L3-3.5.3e *Block Untrusted Assets*	Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile.

INCIDENT RESPONSE (IR)

Level 2	Description
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	Description
IR.L3-3.6.1e *Security Operations Center*	Establish and maintain a security operations center capability that operates 24/7, with allowance for remote/on-call staff.
IR.L3-3.6.2e *Cyber Incident Response Team*	Establish and maintain a cyber incident response team that can be deployed by the organization within 24 hours.

MAINTENANCE (MA)

Level 2	Description
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*	Sanitize equipment removed for off-site maintenance 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.

MEDIA PROTECTION (MP)

Level 1

Level 1	Description
MP.L1-b.1.vii *Media Disposal [FCI Data]*	Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

Level 2

Level 2	Description
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.L2-3.8.3 *Media Disposal [CUI Data]*	Sanitize or destroy system media containing CUI before disposal or release for reuse.
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.

PERSONNEL SECURITY (PS)

Level 2

Level 2	Description
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*	Protect organizational systems containing CUI during and after personnel actions such as terminations and transfers.

Level 3	Description
PS.L3-3.9.2e *Adverse Information*	Protect organizational systems when adverse information develops or is obtained about individuals with access to CUI.

PHYSICAL PROTECTION (PE)

Level 1	Description
PE.L1-b.1.viii *Limit Physical Access [FCI Data]*	Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
PE.L1-b.1.ix *Manage Visitors & Physical Access [FCI Data]*	Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

Level 2	Description
PE.L2-3.10.1 *Limit Physical Access [CUI Data]*	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.
PE.L2-3.10.2 *Monitor Facility*	Protect and monitor the physical facility and support infrastructure for organizational systems.
PE.L2-3.10.3 *Escort Visitors [CUI Data]*	Escort visitors and monitor visitor activity.
PE.L2-3.10.4 *Physical Access Logs [CUI Data]*	Maintain audit logs of physical access.
PE.L2-3.10.5 *Manage Physical Access [CUI Data]*	Control and manage physical access devices.
PE.L2-3.10.6 *Alternative Work Sites*	Enforce safeguarding measures for CUI at alternate work sites.

RISK ASSESSMENT (RA)

Level 2	Description
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	Description
RA.L3-3.11.1e *Threat-Informed Risk Assessment*	Employ threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.
RA.L3-3.11.2e *Threat Hunting*	Conduct cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.
RA.L3-3.11.3e *Advanced Risk Identification*	Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components.
RA.L3-3.11.4e *Security Solution Rationale*	Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.
RA.L3-3.11.5e *Security Solution Effectiveness*	Assess the effectiveness of security solutions at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.
RA.L3-3.11.6e *Supply Chain Risk Response*	Assess, respond to, and monitor supply chain risks associated with organizational systems and system components.
RA.L3-3.11.7e *Supply Chain Risk Plan*	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident.

SECURITY ASSESSMENT (CA)

Level 2	Description
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 *Operational 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 determine 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	Description
CA.L3-3.12.1e *Penetration Testing*	Conduct penetration testing at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests using subject matter experts.

SYSTEM AND COMMUNICATIONS PROTECTION (SC)

Level 1	Description
SC.L1-b.1.x *Boundary Protection [FCI Data]*	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-b.1.xi *Public-Access System Separation [FCI Data]*	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

Level 2	Description
SC.L2-3.13.1 *Boundary Protection [CUI Data]*	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.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.L2-3.13.5 *Public-Access System Separation [CUI Data]*	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
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	Description
SC.L3-3.13.4e *Isolation*	Employ physical isolation techniques or logical isolation techniques or both in organizational systems and system components.

SYSTEM AND INFORMATION INTEGRITY (SI)

Level 1	Description
SI.L1-b.1.xii *Flaw Remediation [FCI Data]*	Identify, report, and correct information and information system flaws in a timely manner.
SI.L1-b.1.xiii *Malicious Code Protection [FCI Data]*	Provide protection from malicious code at appropriate locations within organizational information systems.
SI.L1-b.1.xiv *Update Malicious Code Protection [FCI Data]*	Update malicious code protection mechanisms when new releases are available.
SI.L1-b.1.xv *System & File Scanning [FCI Data]*	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	Description
SI.L2-3.14.1 *Flaw Remediation [CUI Data]*	Identify, report, and correct system flaws in a timely manner.
SI.L2-3.14.2 *Malicious Code Protection [CUI Data]*	Provide protection from malicious code at designated locations within organizational systems.

SI.L2-3.14.3 *Security Alerts & Advisories*	Monitor system security alerts and advisories and take action in response.
SI.L2-3.14.4 *Update Malicious Code Protection [CUI Data]*	Update malicious code protection mechanisms when new releases are available.
SI.L2-3.14.5 *System & File Scanning [CUI Data]*	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.
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	Description
SI.L3-3.14.1e *Integrity Verification*	Verify the integrity of security critical and essential software using root of trust mechanisms or cryptographic signatures.
SI.L3-3.14.3e *Specialized Asset Security*	Include specialized assets such as IoT, IIoT, OT, GFE, Restricted Information Systems and test equipment in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.
SI.L3-3.14.6e *Threat-Guided Intrusion Detection*	Use threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources, and any DoD-provided sources, to guide and inform intrusion detection and threat hunting.

Appendix A. CMMC Model Matrix

This appendix presents the model in matrix form by domain. The three columns list the associated security requirements for each CMMC level. Each level is independent and consists of a set of CMMC security requirements:

- Level 1: the *basic safeguarding requirements* for FCI specified in FAR Clause 52.204-21.
- Level 2: the *security requirements* for CUI specified in NIST SP 800-171 Rev 2 per DFARS Clause 252.204-7012
- Level 3: selected *enhanced security requirements* for CUI specified in NIST SP 800-172 with DoD-approved parameters where applicable.

Each requirement is contained in a single cell. The requirement identification number is bolded at the top of each cell. The next line contains the requirement short name identifier, in *italics*, which is meant to be used for quick reference only. Below the short name is the complete CMMC security requirement statement. Some Level 3 requirement statements contain a DoD-approved parameter, which is underlined. 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
AC.L1-b.1.i *Authorized Access Control [FCI Data]* 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.L2-3.1.1** *Authorized Access Control [CUI Data]* Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). • NIST SP 800-171 Rev 2 3.1.1 • FAR Clause 52.204-21 b.1.i	**AC.L3-3.1.2e** *Organizationally Controlled Assets* Restrict access to systems and system components to only those information resources that are owned, provisioned, or issued by the organization. • NIST SP 800-172 3.1.2e
AC.L1-b.1.ii *Transaction & Function Control [FCI Data]* 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.L2-3.1.2** *Transaction & Function Control [CUI Data]* Limit system access to the types of transactions and functions that authorized users are permitted to execute. • NIST SP 800-171 Rev 2 3.1.2 • FAR Clause 52.204-21 b.1.ii	**AC.L3-3.1.3e** *Secured Information Transfer* Employ secure information transfer solutions to control information flows between security domains on connected systems. • NIST SP 800-172 3.1.3e
AC.L1-b.1.iii *External Connections [FCI Data]* 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.L2-3.1.3** *Control CUI Flow* Control the flow of CUI in accordance with approved authorizations. • NIST SP 800-171 Rev 2 3.1.3	
AC.L1-b.1.iv *Control Public Information [FCI Data]* 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.L2-3.1.4** *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.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.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	

Level 1	Level 2	Level 3
	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	
	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.L2-3.1.20 *External Connections [CUI Data]* Verify and control/limit connections to and use of external systems. • NIST SP 800-171 Rev 2 3.1.20 • FAR Clause 52.204-21 b.1.iii	

Level 1	Level 2	Level 3
	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	
	AC.L2-3.1.22 *Control Public Information [CUI Data]* Control CUI posted or processed on publicly accessible systems. • NIST SP 800-171 Rev 2 3.1.22 • FAR Clause 52.204-21 b.1.iv	

AWARENESS AND TRAINING (AT)

Level 1	Level 2	Level 3
	AT.L2-3.2.1 *Role-Based Risk Awareness* Inform managers, systems administrators, and users of organizational systems 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.L3-3.2.1e** *Advanced Threat Awareness* Provide awareness training upon initial hire, following a significant cyber event, and at least annually, 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. • NIST SP 800-172 3.2.1e
	AT.L2-3.2.2 *Role-Based Training* Train personnel to carry out their assigned information security-related duties and responsibilities. • NIST SP 800-171 Rev 2 3.2.2	**AT.L3-3.2.2e** *Practical Training Exercises* Include practical exercises in awareness training for all users, tailored by roles, to include general users, users with specialized roles, and privileged users, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors. • NIST SP 800-172 3.2.2e
	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
	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* Uniquely track the actions of individual system 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
-	**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.L3-3.4.1e** *Authoritative Repository* Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components. • NIST SP 800-172 3.4.1e
-	**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.L3-3.4.2e** *Automated Detection & Remediation* Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, remove the components or place the components in a quarantine or remediation network to facilitate patching, re-configuration, or other mitigations. • NIST SP 800-172 3.4.2e
	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.L3-3.4.3e** *Automated Inventory* Employ automated discovery and management tools to maintain an up-to-date, complete, accurate, and readily available inventory of system components. • NIST SP 800-172 3.4.3e
	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	

Level 1	Level 2	Level 3
	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
IA.L1-b.1.v *Identification [FCI Data]* 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.L2-3.5.1** *Identification [CUI Data]* Identify system users, processes acting on behalf of users, and devices. • NIST SP 800-171 Rev 2 3.5.1 • FAR Clause 52.204-21 b.1.v	**IA.L3-3.5.1e** *Bidirectional Authentication* Identify and authenticate systems and system components, where possible, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant. • NIST SP 800-172 3.5.1e
IA.L1-b.1.vi *Authentication [FCI Data]* 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.L2-3.5.2** *Authentication [CUI Data]* Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems. • NIST SP 800-171 Rev 2 3.5.2 • FAR Clause 52.204-21 b.1.vi	**IA.L3-3.5.3e** *Block Untrusted Assets* Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state, or in a trust profile. • NIST SP 800-172 3.5.3e
	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.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	

Level 1	Level 2	Level 3
	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
	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.L3-3.6.1e** *Security Operations Center* Establish and maintain a security operations center capability that operates 24/7, with allowance for remote/on-call staff. • NIST SP 800-172 3.6.1e
	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.L3-3.6.2e** *Cyber Incident Response Team* Establish and maintain a cyber incident response team that can be deployed by the organization within 24 hours. • NIST SP 800-172 3.6.2e
	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
-	**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* Sanitize equipment removed for off-site maintenance 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
MP.L1-b.1.vii *Media Disposal [FCI Data]* 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.L2-3.8.3 *Media Disposal [CUI Data]* Sanitize or destroy system media containing CUI before disposal or release for reuse. • NIST SP 800-171 Rev 2 3.8.3 • FAR Clause 52.204-21 b.1.vii	
	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
	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.L3-3.9.2e** *Adverse Information* Protect organizational systems when adverse information develops or is obtained about individuals with access to CUI. • NIST SP 800-172 3.9.2e
	PS.L2-3.9.2 *Personnel Actions* Protect organizational systems containing CUI 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
PE.L1-b.1.viii *Limit Physical Access [FCI Data]* 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.L2-3.10.1** *Limit Physical Access [CUI Data]* Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals. • NIST SP 800-171 Rev 2 3.10.1 • FAR Clause 52.204-21 b.1.viii	
PE.L1-b.1.ix *Manage Visitors & Physical Access [FCI Data]* Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices. • FAR Clause 52.204-21 Partial b.1.ix • NIST SP 800-171 Rev 2 3.10.3 • NIST SP 800-171 Rev 2 3.10.4 • NIST SP 800-171 Rev 2 3.10.5	**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.L2-3.10.3 *Escort Visitors [CUI Data]* Escort visitors and monitor visitor activity. • NIST SP 800-171 Rev 2 3.10.3 • FAR Clause 52.204-21 Partial b.1.ix	
	PE.L2-3.10.4 *Physical Access Logs [CUI Data]* Maintain audit logs of physical access. • NIST SP 800-171 Rev 2 3.10.4 • FAR Clause 52.204-21 Partial b.1.ix	
	PE.L2-3.10.5 *Manage Physical Access [CUI Data]* Control and manage physical access devices. • NIST SP 800-171 Rev 2 3.10.5 • FAR Clause 52.204-21 Partial b.1.ix	
	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	

RISK ASSESSMENT (RA)

Level 1	Level 2	Level 3
	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.L3-3.11.1e** *Threat-Informed Risk Assessment* Employ threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities. • NIST SP 800-172 3.11.1e
	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.L3-3.11.2e** *Threat Hunting* Conduct cyber threat hunting activities on an on-going aperiodic basis or when indications warrant, to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls. • NIST SP 800-172 3.11.2e
	RA.L2-3.11.3 *Vulnerability Remediation* Remediate vulnerabilities in accordance with risk assessments. • NIST SP 800-171 Rev 2 3.11.3	**RA.L3-3.11.3e** *Advanced Risk Identification* Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems, and system components. • NIST SP 800-172 3.11.3e
		RA.L3-3.11.4e *Security Solution Rationale* Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination. • NIST SP 800-172 3.11.4e
		RA.L3-3.11.5e *Security Solution Effectiveness* Assess the effectiveness of security solutions at least annually or upon receipt of relevant cyber threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence. • NIST SP 800-172 3.11.5e
		RA.L3-3.11.6e *Supply Chain Risk Response* Assess, respond to, and monitor supply chain risks associated with organizational systems and system components. • NIST SP 800-172 3.11.6e

Level 1	Level 2	Level 3
		RA.L3-3.11.7e *Supply Chain Risk Plan* Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident. • NIST SP 800-172 3.11.7e

SECURITY ASSESSMENT (CA)

Level 1	Level 2	Level 3
	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.L3-3.12.1e** *Penetration Testing* Conduct penetration testing at least annually or when significant security changes are made to the system, leveraging automated scanning tools and ad hoc tests using subject matter experts. • NIST SP 800-172 3.12.1e
	CA.L2-3.12.2 *Operational 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 determine 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
SC.L1-b.1.x *Boundary Protection [FCI Data]* 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.L2-3.13.1** *Boundary Protection [CUI Data]* 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. • NIST SP 800-171 Rev 2 3.13.1 • FAR Clause 52.204-21 b.1.x	**SC.L3-3.13.4e** *Isolation* Employ physical isolation techniques or logical isolation techniques or both in organizational systems and system components. • NIST SP 800-172 3.13.4e
SC.L1-b.1.xi *Public-Access System Separation [FCI Data]* 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.L2-3.13.2** *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.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.L2-3.13.5 *Public-Access System Separation [CUI Data]* Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. • NIST SP 800-171 Rev 2 3.13.5 • FAR Clause 52.204-21 b.1.xi	
	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	

Level 1	Level 2	Level 3
	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	
	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
SI.L1-b.1.xii *Flaw Remediation [FCI Data]* 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.L2-3.14.1** *Flaw Remediation [CUI Data]* Identify, report, and correct system flaws in a timely manner. • NIST SP 800-171 Rev 2 3.14.1 • FAR Clause 52.204-21 b.1.xii	**SI.L3-3.14.1e** *Integrity Verification* Verify the integrity of security critical and essential software using root of trust mechanisms or cryptographic signatures. • NIST SP 800-172 3.14.1e
SI.L1-b.1.xiii *Malicious Code Protection [FCI Data]* 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.L2-3.14.2** *Malicious Code Protection [CUI Data]* Provide protection from malicious code at designated locations within organizational systems. • NIST SP 800-171 Rev 2 3.14.2 • FAR Clause 52.204-21 b.1.xiii	**SI.L3-3.14.3e** *Specialized Asset Security* Include specialized assets such as IoT, IIoT, OT, GFE, Restricted Information Systems and test equipment in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks. • NIST SP 800-172 3.14.3e
SI.L1-b.1.xiv *Update Malicious Code Protection [FCI Data]* 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.L2-3.14.3** *Security Alerts & Advisories* Monitor system security alerts and advisories and take action in response. • NIST SP 800-171 Rev 2 3.14.3	**SI.L3-3.14.6e** *Threat-Guided Intrusion Detection* Use threat indicator information and effective mitigations obtained from, at a minimum, open or commercial sources, and any DoD-provided sources, to guide and inform intrusion detection and threat hunting. • NIST SP 800-172 3.14.6e
SI.L1-b.1.xv *System & File Scanning [FCI Data]* 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	**SI.L2-3.14.4** *Update Malicious Code Protection [CUI Data]* Update malicious code protection mechanisms when new releases are available. • NIST SP 800-171 Rev 2 3.14.4 • FAR Clause 52.204-21 b.1.xiv	
	SI.L2-3.14.5 *System & File Scanning [CUI Data]* Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed. • NIST SP 800-171 Rev 2 3.14.5 • FAR Clause 52.204-21 b.1.xv	
	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.L2-3.14.7 *Identify Unauthorized Use* Identify unauthorized use of organizational systems. • NIST SP 800-171 Rev 2 3.14.7	

Appendix B. Abbreviations and Acronyms

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

AC	Access Control
APT	Advanced Persistent Threat
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment
CFR	Code of Federal Regulations
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
IA	Identification and Authentication
IR	Incident Response
L#	Level Number
MA	Maintenance
MP	Media Protection
N/A	Not Applicable (NA)
NIST	National Institute of Standards and Technology
OUSD A&S	Office of the Under Secretary of Defense for Acquisition and Sustainment
PE	Physical Protection
PS	Personnel Security
PUB	Publication
Rev	Revision
RA	Risk Assessment
SC	System and Communications Protection
SI	System and Information Integrity
SP	Special Publication
UARC	University Affiliated Research Center

U.S.	United States
VoIP	Voice over Internet Protocol
Vol.	Volume

Appendix C. 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. 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

This page intentionally left blank.


DEPARTMENT OF DEFENSE
CHIEF INFORMATION OFFICER
CYBERSECURITY MATURITY MODEL
CERTIFICATION