C2M2 | Cybersecurity Capability Maturity Model

# C2M2–CMMC Supplemental Guidance

## A Guide for Users of the Cybersecurity Capability Maturity Model (C2M2) and Cybersecurity Maturity Model Certification (CMMC)

January 2024

U.S. DEPARTMENT OF ENERGY

*Office of* Cybersecurity, Energy Security, and Emergency Response

# TABLE OF CONTENTS

# LIST OF TABLES

# ACKNOWLEDGEMENTS

This guidance document was developed through a collaborative effort between public- and private-sector organizations, sponsored by the United States Department of Energy (DOE), the Electricity Subsector Coordinating Council (ESCC), and the Oil and Natural Gas Subsector Coordinating Council (ONG SCC). The DOE thanks the organizations and individuals who provided the critiques, evaluations, and recommendations necessary to produce this document.

## Subgroup Co-Leads

**Shawn Bilak**
Southern Company

**Kaitlin Brennan**
Edison Electric Institute

**Moin Shaikh**
Long Island Power Authority

## Subgroup Members and Contributors

Joseph Adams, Duke Energy

Brian Benestelli, Carnegie Mellon University Software Engineering Institute - CERT Program

Stacy Bostjanick, Chief DIB Cybersecurity, United States Department of Defense CIO

Rich Caralli, Axio

Eric Cardwell, Axio

Jack Cashin, American Public Power Association

Pamela Curtis, Axio

Buddy Dees, Director, CMMC, United States Department of Defense CIO

Andrew Fitzgerald, Exelon

Tricia Flinn, Carnegie Mellon University Software Engineering Institute - CERT Program

John Fry, Axio

Doug Gardner, Carnegie Mellon University Software Engineering Institute - CERT Program

James Gillooley, Lead, CMMC Requirements, United States Department of Defense CIO

Aaron Hescox, Exelon

Alex Hofmann, American Public Power Association

William Hutton, National Rural Electric Cooperative Association

Gavin T Jurecko, Carnegie Mellon University Software Engineering Institute - CERT Program

Daniel Kambic, Carnegie Mellon University Software Engineering Institute - CERT Program

Ismael Khokhar, ICF

Lindsay Kishter, Nexight

Annabelle Lee, Nevermore Security

Jim Linn, American Gas Association / Downstream Natural Gas Information Sharing and Analysis Center

Jacob Maenner, Exelon

Dana Mason, Lead, CMMC Operations, United States Department of Defense CIO

Fowad Muneer, United States Department of Energy

Michael Perdunn, Omaha Public Power District

Alexander Petrilli, Carnegie Mellon University Software Engineering Institute - CERT Program

Vijay Pounraj, CPS Energy

Frank Smith, Carnegie Mellon University Software Engineering Institute - CERT Program

Emma Stewart, National Rural Electric Cooperative Association

Ryan Subers, Axio

Darlene Thorsen, Pacific Northwest National Laboratory

Stephanie Toussaint, Edison Electric Institute

# 1. INTRODUCTION

The Cybersecurity Capability Maturity Model (C2M2) focuses on the implementation and management of cybersecurity practices associated with information technology (IT), operations technology (OT), and information assets and the environments in which they operate. The model can potentially be used to:

- strengthen organizations' cybersecurity capabilities
- enable organizations to more effectively and consistently evaluate and benchmark cybersecurity capabilities
- share knowledge, best practices, and relevant references across organizations as a means to improve cybersecurity capabilities
- enable organizations to better prioritize actions and investments to improve cybersecurity capabilities

The Department of Energy (DOE) first released C2M2 in 2012 and updated it in 2014 in support of the Electricity Subsector Cybersecurity Risk Management Maturity Initiative, a White House initiative led by the DOE in partnership with the Department of Homeland Security (DHS) and in collaboration with industry, private-sector, and public-sector experts. In 2018, a working group of over 140 energy sector stakeholders started an effort to perform a major update to C2M2, which resulted in version 2.0 being released in 2021. The working group made additional updates to C2M2 in response to feedback received from the public and lessons learned from pilot tests with sector organizations. These changes are reflected in version 2.1 that was released in 2022.

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense (DoD) program designed to strengthen cyber resilience throughout the Defense Industrial Base (DIB), establish common assessment criteria, and help enforce contractual compliance standards in DoD procurements.

The CMMC model is derived largely from three documents:

- *Federal Acquisition Regulation (FAR) 52.204-21 Basic Safeguarding of Covered Contractor Information Systems*
- *NIST Special Publication (SP) 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*; and
- for certain programs, *NIST SP 800-172 Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*.

At the time of writing this document, CMMC is in the process of FAR and DFARS rulemaking, which must be completed before CMMC requirements are included in DoD contracts. The DoD is encouraging companies to implement CMMC in advance of mandatory requirements.

The three levels of CMMC are designed to protect different levels of unclassified material and systems.

- **Level 1** – Focused on protecting Federal Contract Information (FCI), Level 1 has basic requirements listed in the FAR clause 52.204-21, which are aligned to NIST SP 800-171 requirements. Contractors will conduct self-assessments and provide affirmation to compliance at least annually. Third party assessments will not be required.
- **Level 2** – Includes all requirements outlined in NIST SP 800-171 and will apply when adequate safeguarding of CUI is necessary based on applicability of DFARS 252.204-7021. Based on the sensitivity of the CUI to be safeguarded, or the program with which it is associated, Program Managers will specify whether the CMMC Level 2 requirement can be met via contractor self-assessment, or if certification is required. If certification is required, it must be performed by a CMMC third-party assessment organization (C3PAO).
- **Level 3 –** Adds additional controls from NIST SP 800-172 and is designed for the protection of CUI with national security implications. Government assessors will perform Level 3 assessments. Companies seeking a Level 3 assessment must already possess a Level 2 certification.

Although CMMC is not yet in effect, DIB contractors must meet other, related DoD contractual requirements:

- **DFARS 252.204-7012.** This clause has been in effect since 2017 and mandates the application of adequate security for the protection of covered defense information (CDI) through the application of NIST SP 800-171 and requires the reporting of cyber incidents involving CDI or covered contractor information systems.
- **DFARS 252.204-7019** was introduced in November 2020. This clause is a notice of NIST SP 800-171 DoD assessment requirements. It requires contractors to have a current (not older than three years) NIST SP 800-171 DoD assessment on record in Supplier Performance Risk System (SPRS) to be considered for award.
- **DFARS 252.204-7020** was introduced in November 2020. This clause requires contractors to undergo assessment at defined levels (Basic, Medium, High) and to provide access to their facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment.

Because of the alignment of CMMC and the current NIST SP 800-171 DoD requirements, any effort expended for a CMMC certification will directly translate to helping meet the current DFARS requirements. Conversely, addressing a gap with NIST SP 800-171 will help achieve future CMMC compliance requirements.

Despite the obvious overlaps between the current DFARS requirements and the expected CMMC requirements, there are a few notable differences.

- Expect a requirement for open plan of action and milestones (POA&M) items to be closed within 180 days under CMMC. Currently a POA&M can be open indefinitely.

- Under CMMC, some practices must be fully implemented and cannot be included on a POA&M. Currently there are no limits on POA&M items.
- Although POA&Ms will be permitted, a minimum passing score for CMMC is expected.
- C3PAOs using certified assessors will perform CMMC Level 2 assessment certifications. The Government will conduct CMMC Level 3 assessments.

For a full discussion of CMMC and to download the model and other associated guidance, visit the CMMC website.

## Purpose and Audience

This document is published for C2M2 users who are pursuing a CMMC certification to meet DoD contractual requirements. The guidance in this document is intended to help C2M2 users both leverage previous C2M2 experience and identify additional activities that may be necessary to meet CMMC certification requirements. Guidance in this document is written from the perspective of CMMC Level 2 but could also apply to organizations seeking CMMC Level 1.

## Document Organization

- Section 2: Provides background on C2M2 and CMMC and describes key similarities and differences that should be considered by users.
- Section 3: Shows CMMC requirements related to C2M2 practices.
- Appendix A: Describes considerations for C2M2 users that are seeking CMMC certification. This appendix includes the NIST SP 800-171 requirements, the DoD Assessment Methodology point value, along with the CMMC identifier.
- Appendix B: Lists C2M2 practices that may be considered *Fully Implemented* or *Largely Implemented* by organizations that have completed a CMMC assessment.
- Appendix C: Includes references that either were used in the development of this document or provide further information.
- Appendix D: Defines the acronyms used in this document.

## Caution to Readers

Development of this guidance has been coordinated with the DoD CMMC program however, this is only guidance. C2M2 does not have reciprocity with CMMC. C2M2 results cannot be used in place of a CMMC self-assessment or certification.

# 2. CORE CONCEPTS

This chapter describes:

- Several core concepts important for understanding the relationship between C2M2 and CMMC and for properly using this guidance document
- A comparison of the key similarities and differences between C2M2 and CMMC
- Scoping and preparation considerations for C2M2 and CMMC
- C2M2 management activities and SP 800-171 non-federal organization (NFO) controls

Table 1 compares several core concepts of C2M2 and CMMC.

**Table 1: Comparison of Core C2M2 and CMMC Concepts**

| Concept | C2M2 | CMMC |
|---|---|---|
| **Focus** | Indication of cybersecurity and process maturity | Implementation of requirements |
| **Motivation** | Measure cybersecurity program maturity and prioritize improvements | Improve the cyber resilience of the Defense Industrial Base |
| **Application** | Developed by the energy sector, but has broad applicability | Contract requirement for defense contractors |
| **Structure** | Practices organized by domains | Requirements organized by domains |
| **Evaluation Approach** | Voluntary, self-evaluation | Evidence-based assessment (self or third-party) |
| **Scoping** | Typically reflects organizational structure or function performed by the organization | Data-centric (FCI and CUI) |
| **Process Maturity** | Defines indications of institutionalization through the identification of specific cybersecurity management practices | Implementation is measured through the assessment process. |

## Key Similarities and Differences Between C2M2 and CMMC

The cybersecurity activities described in C2M2 and CMMC overlap significantly. Users of both models will find many similar or complementary practices. Both models are focused on practices intended to strengthen an organization's cybersecurity posture. C2M2 and CMMC have structural similarities, such as the logical arrangement of practices into domains. Although both models have scaled levels, there is no direct correlation between the maturity indicator levels (MILs) in C2M2 and the CMMC levels. In C2M2, organizations use MILs to measure the maturity of their cybersecurity capabilities, as well as the level of institutionalization (i.e., how ingrained the capabilities are in an organization's operations). The levels in CMMC are sets of cybersecurity requirements that align with the basic safeguarding requirements for FCI and security requirements for CUI. These levels do not directly measure the institutionalization of an organization's activities.

As noted earlier, the DoD created CMMC to strengthen the cyber resilience of the DIB in response to targeting by threat actors. Protecting sensitive information within the defense supply chain is of vital national importance and helps the United States maintain strategic advantage. Similarly, critical infrastructure operators are responsible for delivering essential goods and services, such as the transmission of electricity and distribution of natural gas. The DOE created C2M2 to provide organizations with a method to evaluate and plan cybersecurity program improvements. Although created by the energy sector, C2M2 applies across a wide range of sectors.

Organizations use the C2M2 primarily to

- measure the current state of their cybersecurity capabilities;
- identify gaps between their current state and a defined target state; and
- plan improvements that will enable them to reach their target state.

Organizations may choose to implement the practices in CMMC as a means of implementing best practices for protecting information. However, they would likely be seeking CMMC certification as part of meeting necessary requirements when contracting with the DoD.

## Self-Evaluation Scoping and Preparation Considerations

A critical step in any evaluation or assessment is the completion of preparation and scoping activities that define criteria. Such activities determine:

- boundaries for an evaluation,
- assets that are within scope,
- subject matter experts that may need to be involved,
- artifacts that may need reviewed, and
- rules of engagement to be followed by those involved in the activities.

Organizations will find that there is significant overlap when preparing to complete a C2M2 self-evaluation or CMMC assessment, but careful consideration should be paid to the differences outlined in the section. Refer to *C2M2 Self-Evaluation Guide*, CMMC assessment guides, and *CMMC Scoping Guidance* for more information.

**Note:** This section compares C2M2 and CMMC. At the time of writing this document, DIB contractors are required to meet only the previously discussed DFARS requirements and may use this information as guidance for planning to meet future CMMC requirements.

### Evaluation Approaches

The C2M2 was designed to be a self-evaluation, during which an organization selects a facilitator who can help guide a workshop of assembled subject matter experts (SMEs). For each practice, SMEs provide a consensus response regarding the level of implementation of cybersecurity activities. Organizations that choose to use C2M2 to evaluate their cybersecurity capabilities may use the results to plan improvements.

In contrast, DIB contractors will be required to meet CMMC requirements as a condition of contract or option year award. The CMMC certification level that an organization is required to achieve is based on the sensitivity of the information to be safeguarded, or the program with which it is associated. The following table compares CMMC levels and assessment types.

Table 2: Comparison of CMMC Levels and Assessment Types

| CMMC Level | Type of Information Being Safeguarded | Assessment Type |
|---|---|---|
| Level 1 | Federal Contract Information | Self-assessment |
| Level 2 | Controlled Unclassified Information | Self-assessment |
| | Controlled Unclassified Information critical to national security | Third-Party Assessment |
| Level 3 | Controlled Unclassified Information critical to national security | Third-Party Assessment |

Another key difference between C2M2 and CMMC is the assessment methodology. C2M2 self-evaluation tools capture workshop participant responses for the implementation level of each of practice through a facilitated one-day workshop. Preparation for a C2M2 self-evaluation typically includes the determination of the scope, selection of workshop participants, and handling of workshop logistics.

Additional time and resources are necessary to prepare for a CMMC assessment because it requires evidence to substantiate the implementation of the assessment objectives for each requirement. If an organization is subject to a third-party assessment, it may refer to the potential assessment methods and objects in the corresponding *CMMC Assessment Guide* for additional information regarding what an assessor may request to examine and test, along with individuals that may be interviewed. There is no requirement to use the guides. Organizations can use NIST SP 800-171A or other tools to assist in preparation for a third-party assessment. Similar documentation is necessary even if an organization completes a self-assessment (e.g., System Security Plan (SSP), network diagram, POA&M). Regardless of the type of CMMC assessment, it is important for organizations to consider the individual assessment objectives of each CMMC requirement. At Level 2, the NIST SP 800-171 requirements have assessment objectives that would be evaluated by an assessor.

### Scoping

Prior to conducting a C2M2 self-evaluation workshop, an organization should determine the scope–known as the function–of the self-evaluation. The function is used as an input into selection of self-evaluation participants and assets to be considered when selecting implementation level responses for each practice. Organizations have flexibility when

choosing the function, and may choose a very focused scope, such as electric generation, or scope the function at a higher organizational or enterprise level.

Organizational structure or services that an organization performs drive C2M2 scoping. Scoping for a CMMC assessment requires a data-centric approach. Since DIB contractors have a responsibility to protect the confidentiality of FCI and CUI, they must complete scoping based upon where this sensitive information is processed, stored, and transmitted. Based on various factors, such as organization size, business type, and services offered, organizations may choose to physically or logically separate FCI and CUI, which may reduce the scope of the CMMC assessment. Conversely, it may not be feasible to implement such separations, so an organization may choose an enterprise-level scope.

The selection of the function for a C2M2 self-evaluation, or the assessment scope for CMMC, determines the assets that an organization must consider. The C2M2 model covers all information technology (IT), operational technology (OT), and information assets used for the delivery of the function or that could impact the function if compromised by an attacker. CMMC takes a similar approach, but an organization should carefully consider the requirements for the defined asset categories detailed in *CMMC Scoping Guidance*. In-scope CMMC assessment assets include those that process, store, or transmit CUI, security protection assets, contractor risk-managed assets, and specialized assets. All assets must be documented in three locations: in an asset inventory, in the contractor's SSP, and in a network diagram.

Contractor risk-managed assets and specialized assets are reviewed during an assessment to ensure that the contractor has sufficient risk-based policies, procedures, and practices. However, these assets are not assessed against the CMMC requirements. Contractor risk managed assets include assets that can, but are not intended to, process, store, or transmit CUI. Specialized assets include assets that may or may not process, store, or transmit CUI. These include internet-of-things (IoT) devices, OT assets, restricted information systems, and test equipment. For an asset to be considered outside the scope of a CMMC assessment, it must be physically or logically separated from CUI assets.

### Documentation

As mentioned previously, additional time and effort may be necessary to prepare for a CMMC assessment. Specific documentation, such as an SSP, asset inventory, and a network diagram, is required documentation that an assessor will review. Examples of additional documentation that may be examined for each CMMC requirement are detailed in the *CMMC Assessment Guide*.

CMMC documentation requirements differ from those necessary to complete a C2M2 self-evaluation. Some C2M2 practices describe the implementation of policies or procedures but, because a C2M2 self-evaluation is not evidence-based, an organization is not required to substantiate its practice responses an artifact. When preparing for a CMMC assessment, organizations may find they have similar documentation in place already but should review the *CMMC Assessment Guide* to determine additional documentation that may be necessary in preparation for a CMMC assessment. For example, an organization may have

documented the implementation of security controls, but this documentation may need to be adapted to develop an SSP.

## C2M2 Management Activities and NIST SP 800-171 Revision 2 NFO Controls

C2M2 is a dual-progression maturity model that measures both the implementation of cybersecurity capabilities, as well as the level to which these capabilities are ingrained in an organization's operations, called "institutionalization." A similar set of practices in each C2M2 domain, called Management Activities, measure the performance of the activities that institutionalize the domain-specific practices. For example, implementing procedures and providing adequate resources to complete domain-specific activities increases an organization's confidence that such activities will be performed consistently, even in times of stress. Organizations should consider the tailoring criteria used in the development of NIST SP 800-171 Revision 2. Appendix E of NIST SP 800-171 Revision 2 includes details of these criteria, as well as controls or control enhancements that are "expected to be routinely satisfied by nonfederal organizations without specification." The controls include policies, procedures, and other documents that have been tailored out of the NIST SP 800-53 moderate baseline, which was the basis for the CUI-derived security requirements.

# 3. APPLYING C2M2 TO CMMC

This section shows CMMC requirements that have a relationship with C2M2 practices. This section may be used in conjunction with a C2M2 self-evaluation or the results of a C2M2 self-evaluation to gain an understanding of how an organization's C2M2 results might compare to implementation of CMMC requirements.

**Note:** In the tables below, click the CMMC requirement identifier shown in blue in square brackets in the right column (e.g., [AC.L2-3.1.16]) to view more information about the associated CMMC requirement in *Appendix A: CMMC Assessment Considerations*.

## Asset, Change, and Configuration Management (ASSET)

*Purpose: Manage the organization's IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objectives.*

**Objectives and Practices**

### 1. Manage IT and OT Asset Inventory

| | | | |
|---|---|---|---|
| MIL1 | a. | IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner | [AC.L2-3.1.16] |
| MIL2 | b. | The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective | |
| | c. | Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function | |
| | d. | Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective | |
| | e. | The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system, and firmware versions) | |
| MIL3 | f. | The IT and OT asset inventory is complete (the inventory includes all assets within the function) | [CM.L2-3.4.1] |
| | g. | The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes | |
| | h. | Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life | [MA.L2-3.7.3] [MP.L2-3.8.3] |

## 2. Manage Information Asset Inventory

| | | | |
|---|---|---|---|
| MIL1 | a. | Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner | |
| MIL2 | b. | The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective | |
| | c. | Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function | |
| | d. | Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective | |
| | e. | The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements) | [PE.L2-3.10.6] |
| MIL3 | f. | The information asset inventory is complete (the inventory includes all assets within the function) | [CM.L2-3.4.1] |
| | g. | The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes | |
| | h. | Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements | [MP.L2-3.8.3] |

## 3. Manage IT and OT Asset Configuration

| | | | |
|---|---|---|---|
| MIL1 | a. | **Configuration baselines are established, at least in an ad hoc manner** | **[CM.L2-3.4.1]** |
| MIL2 | b. | **Configuration baselines are used to configure assets at deployment and restoration** | |
| | c. | **Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f)** | **[CM.L2-3.4.2] [CM.L2-3.4.9] [SC.L2-3.13.9]** |
| | d. | **Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture** | |
| MIL3 | e. | **Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles** | **[CM.L2-3.4.1] [CM.L2-3.4.2] [CM.L2-3.4.9]** |

## 4. Manage Changes to IT and OT Assets

| | | | |
|---|---|---|---|
| MIL1 | a. | **Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner** | **[CM.L2-3.4.3] [MA.L2-3.7.2]** |
| | b. | **Changes to assets are documented, at least in an ad hoc manner** | **[CM.L2-3.4.3]** |
| MIL2 | c. | **Documentation requirements for asset changes are established and maintained** | |
| | d. | Changes to higher priority assets are tested prior to being deployed | |
| | e. | Changes and updates are implemented in a secure manner | [CM.L2-3.4.5] [MA.L2-3.7.5] |
| | f. | The capability to reverse changes is established and maintained for assets that are important to the delivery of the function | |
| | g. | Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement) | [CM.L2-3.4.3] |
| MIL3 | h. | Changes to higher priority assets are tested for cybersecurity impact prior to being deployed | [CM.L2-3.4.4] |
| | i. | Change logs include information about modifications that impact the cybersecurity requirements of assets | [CM.L2-3.4.3] |

## 5. Management Activities for the ASSET Domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the ASSET domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the ASSET domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel |
| | e. | Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the ASSET domain is evaluated and tracked |

## Threat and Vulnerability Management (THREAT)

*Purpose: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives.*

### Objectives and Practices

### 1. Reduce Cybersecurity Vulnerabilities

| | | | |
|---|---|---|---|
| MIL1 | a. | Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner | [SI.L2-3.14.1] |
| | b. | Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner | [SI.L2-3.14.1] [SI.L2-3.14.3] |
| | c. | Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner | [RA.L2-3.11.3] [SI.L2-3.14.1] |
| | d. | Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner | [RA.L2-3.11.3] [SI.L2-3.14.1] |
| MIL2 | e. | Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored | |
| | f. | Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events | [RA.L2-3.11.2] |
| | g. | Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly | [RA.L2-3.11.3] [SI.L2-3.14.3] |
| | h. | Operational impact to the function is evaluated prior to deploying patches or other mitigations | |
| | i. | Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders | |
| MIL3 | j. | Cybersecurity vulnerability information sources that collectively address all IT and OT assets within the function are monitored | |
| | k. | Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function | |
| | l. | Vulnerability monitoring activities include review to confirm that actions taken in response to cybersecurity vulnerabilities were effective | |
| | m. | Mechanisms are established and maintained to receive and respond to reports from the public or external parties of potential vulnerabilities related to the organization's IT and OT assets, such as public-facing websites or mobile applications | [RA.L2-3.11.3] |

## 2. Respond to Threats and Share Threat Information

| | | | |
|---|---|---|---|
| MIL1 | a. | Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner | |
| | b. | Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner | [SI.L2-3.14.3] |
| | c. | Threat objectives for the function are identified, at least in an ad hoc manner | |
| | d. | Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner | |
| MIL2 | e. | A threat profile for the function is established that includes threat objectives and additional threat characteristics (for example, threat actor types, motives, capabilities, and targets) | |
| | f. | Threat information sources that collectively address all components of the threat profile are prioritized and monitored | |
| | g. | Identified threats are analyzed and prioritized and are addressed accordingly | [SI.L2-3.14.3] |
| | h. | Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs]) | |
| MIL3 | i. | The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events | |
| | j. | Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g) | |
| | k. | Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action | |

## 3. Management Activities for the THREAT Domain

| | | | |
|---|---|---|---|
| MIL1 | No practice at MIL1 | | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the THREAT domain | [SI.L2-3.14.3] |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain | |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the THREAT domain | |
| | d. | Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel | |
| | e. | Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities | |
| | f. | The effectiveness of activities in the THREAT domain is evaluated and tracked | |

## Risk Management (RISK)

*Purpose: Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.*

Objectives and Practices

### 1. Establish and Maintain Cyber Risk Management Strategy and Program

| | | |
|---|---|---|
| MIL1 | a. | The organization has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner |
| MIL2 | b. | A strategy for cyber risk management is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture |
| | c. | The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy |
| | d. | Information from RISK domain activities is communicated to relevant stakeholders |
| | e. | Governance for the cyber risk management program is established and maintained |
| | f. | Senior management sponsorship for the cyber risk management program is visible and active |
| MIL3 | g. | The cyber risk management program aligns with the organization's mission and objectives |
| | h. | The cyber risk management program is coordinated with the organization’s enterprise-wide risk management program |

## 2. Identify Cyber Risk

| | | | |
|---|---|---|---|
| MIL1 | a. | Cyber risks are identified, at least in an ad hoc manner | |
| MIL2 | b. | A defined method is used to identify cyber risks | [RA.L2-3.11.1] |
| | c. | Stakeholders from appropriate operations and business areas participate in the identification of cyber risks | |
| | d. | Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level | |
| | e. | Cyber risk categories and cyber risks are documented in a risk register or other artifact | |
| | f. | Cyber risk categories and cyber risks are assigned to risk owners | |
| | g. | Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events | [RA.L2-3.11.1] |
| MIL3 | h. | Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction | [RA.L2-3.11.1] |
| | i. | Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities) | [CA.L2-3.12.2] |
| | j. | Threat management information from THREAT domain activities is used to update cyber risks and identify new risks | |
| | k. | Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks | |
| | l. | Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks | [CA.L2-3.12.2] |
| | m. | Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations | |

## 3. Analyze Cyber Risk

| | | | |
|---|---|---|---|
| MIL1 | a. | Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner | |
| MIL2 | b. | Defined criteria are used to prioritize cyber risks (for example, impact to the organization, impact to the community, likelihood, susceptibility, risk tolerance) | |
| | c. | A defined method is used to estimate impact for higher priority cyber risks (for example, comparison to actual events, risk quantification) | |
| | d. | Defined methods are used to analyze higher priority cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility) | |
| | e. | Organizational stakeholders from appropriate operations and business functions participate in the analysis of higher priority cyber risks | |
| | f. | Cyber risks are removed from the risk register or other artifact used to document and manage identified risks when they no longer require tracking or response | |
| MIL3 | g. | Cyber risk analyses are updated periodically and according to defined triggers, such as system changes, external events, and information from other model domains | |

## 4. Respond to Cyber Risk

| | | | |
|---|---|---|---|
| MIL1 | a. | Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner | [CA.L2-3.12.2] |
| MIL2 | b. | A defined method is used to select and implement risk responses based on analysis and prioritization | [CA.L2-3.12.2] |
| MIL3 | c. | Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks | [CA.L2-3.12.1] [CA.L2-3.12.3] |
| | d. | Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated, and risk tolerances are not exceeded | [CA.L2-3.12.3] |
| | e. | Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate | |

## 5. Management Activities for the RISK domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the RISK domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the RISK domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel |
| | e. | Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the RISK domain is evaluated and tracked |

## Identity and Access Management (ACCESS)

*Purpose: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.*

### Objectives and Practices

### 1. Establish Identities and Manage Authentication

| | | | |
|---|---|---|---|
| MIL1 | a. | Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities) | [AC.L2-3.1.4] [IA.L2-3.5.1] |
| | b. | Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner | [AC.L2-3.1.1] [IA.L2-3.5.2] |
| | c. | Identities are deprovisioned, at least in an ad hoc manner, when no longer required | |
| MIL2 | d. | Password strength and reuse restrictions are defined and enforced | [IA.L2-3.5.7] [IA.L2-3.5.8] |
| | e. | Identity repositories are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure | |
| | f. | Identities are deprovisioned within organization-defined time thresholds when no longer required | [IA.L2-3.5.6] [MA.L2-3.7.5] |
| | g. | The use of privileged credentials is limited to processes for which they are required | [AC.L2-3.1.6] |
| | h. | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) | [AC.L2-3.1.2] [AC.L2-3.1.7] [AC.L2-3.1.12] [AC.L2-3.1.15] [AU.L2-3.3.9] [IA.L2-3.5.3] [MA.L2-3.7.5] |
| MIL3 | i. | Multifactor authentication is required for all access, where feasible | |
| | j. | Identities are disabled after a defined period of inactivity, where feasible | [IA.L2-3.5.6] |

## 2. Control Logical Access

| | | | |
|---|---|---|---|
| MIL1 | a. | Logical access controls are implemented, at least in an ad hoc manner | [AC.L2-3.1.1] [AC.L2-3.1.2] [AC.L2-3.1.17] [AC.L2-3.1.18] [CM.L2-3.4.5] [IA.L2-3.5.2] [MA.L2-3.7.2] |
| | b. | Logical access privileges are revoked when no longer needed, at least in an ad hoc manner | [IA.L2-3.5.6] [PS.L2-3.9.2] |
| MIL2 | c. | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) | [AC.L2-3.1.1] [AC.L2-3.1.2] [AC.L2-3.1.7] [AC.L2-3.1.12] [AC.L2-3.1.15] [AC.L2-3.1.16] [AU.L2-3.3.9] [CM.L2-3.4.5] [SC.L2-3.13.3] |
| | d. | Logical access requirements incorporate the principle of least privilege | [AC.L2-3.1.5] |
| | e. | Logical access requirements incorporate the principle of separation of duties | [AC.L2-3.1.4] [SC.L2-3.13.3] |
| | f. | Logical access requests are reviewed and approved by the asset owner | [AC.L2-3.1.15] [AU.L2-3.3.9] |
| | g. | Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring | [AC.L2-3.1.7] [AU.L2-3.3.8] [AU.L2-3.3.9] |
| MIL3 | h. | Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges | |
| | i. | Anomalous logical access attempts are monitored as indicators of cybersecurity events | [SI.L2-3.14.6] [SI.L2-3.14.7] |

## 3. Control Physical Access

| | | | |
|---|---|---|---|
| MIL1 | a. | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner | [CM.L2-3.4.5] [MA.L2-3.7.2] [MP.L2-3.8.1] [MP.L2-3.8.2] [PE.L2-3.10.1] [PE.L2-3.10.2] [PE.L2-3.10.5] |
| | b. | Physical access privileges are revoked when no longer needed, at least in an ad hoc manner | [MP.L2-3.8.2] [PE.L2-3.10.5] |
| | c. | Physical access logs are maintained, at least in an ad hoc manner | [MP.L2-3.8.2] [PE.L2-3.10.4] |
| MIL2 | d. | Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access) | [CM.L2-3.4.5] [MP.L2-3.8.1] [PE.L2-3.10.1] [PE.L2-3.10.5] [PE.L2-3.10.6] |
| | e. | Physical access requirements incorporate the principle of least privilege | |
| | f. | Physical access requirements incorporate the principle of separation of duties | [AC.L2-3.1.4] |
| | g. | Physical access requests are reviewed and approved by the asset owner | |
| | h. | Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring | [PE.L2-3.10.3] |
| MIL3 | i. | Physical access privileges are reviewed and updated | [PE.L2-3.10.5] |
| | j. | Physical access is monitored to identify potential cybersecurity events | [MA.L2-3.7.6] [PE.L2-3.10.2] |

## 4. Management Activities for the ACCESS domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the ACCESS domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the ACCESS domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the ACCESS domain are assigned to personnel |
| | e. | Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the ACCESS domain is evaluated and tracked |

## Situational Awareness (SITUATION)

*Purpose: Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state*

### Objectives and Practices

### 1. Perform Logging

| | | | |
|---|---|---|---|
| MIL1 | a. | Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner | [AC.L2-3.1.7] [AC.L2-3.1.18] [AU.L2-3.3.1] |
| MIL2 | b. | Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible | |
| | c. | Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective | [AC.L2-3.1.7] [AU.L2-3.3.1] [AU.L2-3.3.2] [AU.L2-3.3.3] |
| | d. | Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems) | [AC.L2-3.1.7] [AU.L2-3.3.1] [AU.L2-3.3.2] [AU.L2-3.3.3] |
| | e. | Log data are being aggregated within the function | |
| MIL3 | f. | More rigorous logging is performed for higher priority assets | |

## 2. Perform Monitoring

| | | | |
|---|---|---|---|
| MIL1 | a. | Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner | [AU.L2-3.3.5] [SI.L2-3.14.7] |
| | b. | Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner | [AU.L2-3.3.5] [SI.L2-3.14.7] |
| MIL2 | c. | Monitoring and analysis requirements are established and maintained for the function and address timely review of event data | [AU.L2-3.3.3] [AU.L2-3.3.5] [SI.L2-3.14.6] |
| | d. | Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments | [SI.L2-3.14.6] [SI.L2-3.14.7] |
| | e. | Alarms and alerts are configured and maintained to support the identification of cybersecurity events | [AU.L2-3.3.4] [SI.L2-3.14.6] |
| | f. | Monitoring activities are aligned with the threat profile (THREAT-2e) | |
| MIL3 | g. | More rigorous monitoring is performed for higher priority assets | [AC.L2-3.1.18] |
| | h. | Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity | |
| | i. | Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events | |

## 3. Establish and Maintain Situational Awareness

| | | | |
|---|---|---|---|
| MIL1 | No practice at MIL1 | | |
| MIL2 | a. | Methods of communicating the current state of cybersecurity for the function are established and maintained | |
| | b. | Monitoring data are aggregated to provide an understanding of the operational state of the function | |
| | c. | Relevant information from across the organization is available to enhance situational awareness | |
| MIL3 | d. | Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders | [AU.L2-3.3.5] |
| | e. | Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness | |
| | f. | A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function | [AU.L2-3.3.5] [AU.L2-3.3.6] [SI.L2-3.14.7] |
| | g. | Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains | |

## 4. Management Activities for the SITUATION domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the SITUATION domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the SITUATION domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel |
| | e. | Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the SITUATION domain is evaluated and tracked |

## Event and Incident Response, Continuity of Operations (RESPONSE)

*Purpose: Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.*

### Objectives and Practices

### 1. Detect Cybersecurity Events

| | | | |
|---|---|---|---|
| MIL1 | a. | Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner | [IR.L2-3.6.2] |
| MIL2 | b. | Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events) | |
| | c. | Cybersecurity events are documented based on the established criteria | [AU.L2-3.3.1] |
| MIL3 | d. | Event information is correlated to support incident analysis by identifying patterns, trends, and other common features | |
| | e. | Cybersecurity event detection activities are adjusted based on identified risks and the organization's threat profile (THREAT-2e) | |
| | f. | Situational awareness for the function is monitored to support the identification of cybersecurity events | |

## 2. Analyze Cybersecurity Events and Declare Incidents

| | | | |
|---|---|---|---|
| MIL1 | a. | Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner | [IR.L2-3.6.1] |
| | b. | Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner | |
| MIL2 | c. | Cybersecurity incident declaration criteria are formally established based on the potential impact to the function | |
| | d. | Cybersecurity events are declared to be incidents based on established criteria | |
| | e. | Cybersecurity incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats | |
| | f. | There is a repository where cybersecurity events and incidents are documented and tracked to closure | [IR.L2-3.6.2] |
| | g. | Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d) | [IR.L2-3.6.2] |
| MIL3 | h. | Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b) | |
| | i. | Cybersecurity incidents are correlated to identify patterns, trends, and other common features across multiple incidents | |

## 3. Respond to Cybersecurity Incidents

| | | | |
|---|---|---|---|
| MIL1 | a. | Cybersecurity incident response personnel are identified, and roles are assigned, at least in an ad hoc manner | |
| | b. | Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations | |
| | c. | Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner | [IR.L2-3.6.2] |
| MIL2 | d. | Cybersecurity incident response plans that address all phases of the incident lifecycle are established and maintained | [IR.L2-3.6.1] |
| | e. | Cybersecurity incident response is executed according to defined plans and procedures | [IR.L2-3.6.1] |
| | f. | Cybersecurity incident response plans include a communications plan for internal and external stakeholders | [IR.L2-3.6.2] |
| | g. | Cybersecurity incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events | [IR.L2-3.6.3] |
| | h. | Cybersecurity incident lessons-learned activities are performed, and corrective actions are taken, including updates to the incident response plan | |
| MIL3 | i. | Cybersecurity incident root-cause analysis is performed, and corrective actions are taken, including updates to the incident response plan | |
| | j. | Cybersecurity incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation | |
| | k. | Cybersecurity incident response personnel participate in joint cybersecurity exercises with other organizations | [IR.L2-3.6.3] |
| | l. | Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g) | |

## 4. Address Cybersecurity in Continuity of Operations

| | | | |
|---|---|---|---|
| MIL1 | a. | Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner | |
| | b. | Data backups are available and tested, at least in an ad hoc manner | |
| | c. | IT and OT assets requiring spares are identified, at least in an ad hoc manner | |
| MIL 2 | d. | Continuity plans address potential impacts from cybersecurity incidents | |
| | e. | The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans | |
| | f. | Continuity plans address IT, OT, and information assets that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets | |
| | g. | Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets that are important to the delivery of the function are incorporated into continuity plans | |
| | h. | Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel | |
| | i. | Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events | [IR.L2-3.6.3] |
| | j. | Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data | [MP.L2-3.8.9] |
| | k. | Data backups are logically or physically separated from source data | [MP.L2-3.8.9] |
| | l. | Spares for selected IT and OT assets are available | |
| MIL 3 | m. | Continuity plans are aligned with identified risks and the organization's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats | |
| | n. | Continuity plan exercises address higher priority risks | |
| | o. | The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly | |
| | p. | Continuity plans are periodically reviewed and updated | |

## 5. Management Activities for the RESPONSE domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. Documented procedures are established, followed, and maintained for activities in the RESPONSE domain | |
| | b. Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain | [IR.L2-3.6.1] |
| MIL3 | c. Up-to-date policies or other organizational directives define requirements for activities in the RESPONSE domain | |
| | d. Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel | |
| | e. Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities | |
| | f. The effectiveness of activities in the RESPONSE domain is evaluated and tracked | |

## Third-Party Risk Management (THIRD-PARTIES)

*Purpose: Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.*

### Objectives and Practices

### 1. Identify and Prioritize Third Parties

| | | | |
|---|---|---|---|
| MIL1 | a. | Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner | |
| | b. | Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to the delivery of the function are identified, at least in an ad hoc manner | [MA.L2-3.7.2] |
| MIL2 | c. | A defined method is followed to identify risks arising from suppliers and other third parties | [RA.L2-3.11.1] |
| | d. | Third parties are prioritized according to established criteria (for example, importance to the delivery of the function, impact of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts) | |
| | e. | Escalated prioritization is assigned to suppliers and other third parties whose compromise or disruption could cause significant consequences (for example, single-source suppliers, suppliers with privileged access) | |
| MIL3 | f. | Prioritization of suppliers and other third parties is updated periodically and according to defined triggers, such as system changes and external events | |

## 2. Manage Third-Party Risk

| | | | |
|---|---|---|---|
| MIL1 | a. | The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner | |
| | b. | The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner | |
| MIL2 | c. | A defined method is followed to identify cybersecurity requirements and implement associated controls that protect against the risks arising from suppliers and other third parties | |
| | d. | A defined method is followed to evaluate and select suppliers and other third parties | |
| | e. | More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties | [MA.L2-3.7.2] |
| | f. | Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are formalized in agreements with suppliers and other third parties | |
| | g. | Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements | |
| MIL3 | h. | Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate | |
| | i. | Selection criteria for products include consideration of end-of-life and end-of-support timelines | |
| | j. | Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services | |
| | k. | Selection criteria for higher priority assets include evaluation of bills of material for key asset elements, such as hardware and software | |
| | l. | Selection criteria for higher priority assets include evaluation of any associated third-party hosting environments and source data | |
| | m. | Acceptance testing of procured assets includes consideration of cybersecurity requirements | |

## 3. Management Activities for the THIRD-PARTIES domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the THIRD-PARTIES domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the THIRD-PARTIES domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the THIRD-PARTIES domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel |
| | e. | Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the THIRD-PARTIES domain is evaluated and tracked |

## Workforce Management (WORKFORCE)

*Purpose: Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.*

### Objectives and Practices

### 1. Implement Workforce Controls

| | | | |
|---|---|---|---|
| MIL1 | a. | Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner | [PS.L2-3.9.1] |
| | b. | Personnel separation procedures address cybersecurity, at least in an ad hoc manner | [PS.L2-3.9.2] |
| MIL2 | c. | Personnel vetting is performed at hire and periodically for positions that have access to assets that are important to the delivery of the function | [PS.L2-3.9.1] |
| | d. | Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate | [PS.L2-3.9.2] |
| | e. | Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets | [AC.L2-3.1.22] [AT.L2-3.2.1] |
| MIL3 | f. | Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk | [PS.L2-3.9.1] |
| | g. | A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures | |

### 2. Increase Cybersecurity Awareness

| | | | |
|---|---|---|---|
| MIL1 | a. | Cybersecurity awareness activities occur, at least in an ad hoc manner | |
| MIL2 | b. | Cybersecurity awareness objectives are established and maintained | |
| | c. | Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e) | [AT.L2-3.2.3] |
| | d. | Cybersecurity awareness activities are conducted periodically | [AT.L2-3.2.1] |
| MIL3 | e. | Cybersecurity awareness activities are tailored to job role | [AT.L2-3.2.1] |
| | f. | Cybersecurity awareness activities address predefined states of operation (SITUATION-3g) | |
| | g. | The effectiveness of cybersecurity awareness activities is evaluated periodically and according to defined triggers, such as system changes and external events, and improvements are made as appropriate | |

## 3. Assign Cybersecurity Responsibilities

| | | | |
|---|---|---|---|
| MIL1 | a. | Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner | |
| | b. | Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner | |
| MIL2 | c. | Cybersecurity responsibilities are assigned to specific roles, including external service providers | |
| | d. | Cybersecurity responsibilities are documented | |
| MIL3 | e. | Cybersecurity responsibilities and job requirements are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure | |
| | f. | Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning | |

## 4. Develop Cybersecurity Workforce

| | | | |
|---|---|---|---|
| MIL1 | a. | Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner | [AT.L2-3.2.2] |
| | b. | Cybersecurity knowledge, skill, and ability requirements and gaps are identified for both current and future operational needs, at least in an ad hoc manner | |
| MIL2 | c. | Identified cybersecurity knowledge, skill, and ability gaps are addressed through training, recruiting, and retention efforts | [AT.L2-3.2.2] |
| | d. | Cybersecurity training is provided as a prerequisite to granting access to assets that are important to the delivery of the function | [AT.L2-3.2.2] |
| MIL3 | e. | The effectiveness of training programs is evaluated periodically, and improvements are made as appropriate | |
| | f. | Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities | |

## 5. Management Activities for the WORKFORCE domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the WORKFORCE domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the WORKFORCE domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel |
| | e. | Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the WORKFORCE domain is evaluated and tracked |

## Cybersecurity Architecture (ARCHITECTURE)

*Purpose: Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.*

### Objectives and Practices

### 1. Establish and Maintain Cybersecurity Architecture Strategy and Program

| | | | |
|---|---|---|---|
| MIL1 | a. | The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner | |
| MIL2 | b. | A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture | [CA.L2-3.12.4] |
| | c. | A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization | [CM.L2-3.4.2] [CA.L2-3.12.4] [SC.L2-3.13.2] |
| | d. | Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process | |
| | e. | Senior management sponsorship for the cybersecurity architecture program is visible and active | |
| | f. | The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets | [PE.L2-3.10.6] [CA.L2-3.12.4] [SC.L2-3.13.2] |
| | g. | Cybersecurity controls are selected and implemented to meet cybersecurity requirements | [SC.L2-3.13.2] |
| MIL3 | h. | The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program | |
| | i. | Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events | [CM.L2-3.4.2] [SC.L2-3.13.2] |
| | j. | The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e) | |
| | k. | The cybersecurity architecture addresses predefined states of operation (SITUATION-3g) | |

## 2. Implement Network Protections as an Element of the Cybersecurity Architecture

| | | | |
|---|---|---|---|
| MIL1 | a. | Network protections are implemented, at least in an ad hoc manner | |
| | b. | The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner | |
| MIL2 | c. | Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices) | [AC.L2-3.1.12] [AC.L2-3.1.13] [AC.L2-3.1.14] [SC.L2-3.13.9] |
| | d. | Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements | [SC.L2-3.13.1] [SC.L2-3.13.5] [SC.L2-3.13.3] |
| | e. | Network protections incorporate the principles of least privilege and least functionality | |
| | f. | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) | [AC.L2-3.1.20] [SC.L2-3.13.1] [SC.L2-3.13.6] [SC.L2-3.13.14] [SC.L2-3.13.15] [SI.L2-3.14.2] |
| | g. | Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking) | [SC.L2-3.13.1] [SI.L2-3.14.2] |
| MIL3 | h. | All assets are segmented into distinct security zones based on cybersecurity requirements | [SC.L2-3.13.3] |
| | i. | Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication | |
| | j. | OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems | |
| | k. | Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control (NAC)) | [AC.L2-3.1.16] [AC.L2-3.1.18] |
| | l. | The cybersecurity architecture enables the isolation of compromised assets | |

## 3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

| | | | |
|---|---|---|---|
| MIL1 | a. | Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner | [AC.L2-3.1.1] [AC.L2-3.1.8] [PE.L2-3.10.1] [PE.L2-3.10.5] [SC.L2-3.13.9] |
| | b. | Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner | |
| MIL2 | c. | The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced | [SC.L2-3.13.3] |
| | d. | The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced | [CM.L2-3.4.6] [CM.L2-3.4.7] [CM.L2-3.4.8] [CM.L2-3.4.9] |
| | e. | Secure configurations are established and maintained as part of the asset deployment process where feasible | [AC.L2-3.1.11] [CM.L2-3.4.2] [SC.L2-3.13.4] [SC.L2-3.13.13] |
| | f. | Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls) | [CM.L2-3.4.2] [SC.L2-3.13.7] [SI.L2-3.14.2] |
| | g. | The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) | [AC.L2-3.1.21] [MA.L2-3.7.4] [MP.L2-3.8.7] [MP.L2-3.8.8] |
| | h. | Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible | |
| | i. | Maintenance and capacity management activities are performed for all assets within the function | [MA.L2-3.7.1] |
| | j. | The physical operating environment is controlled to protect the operation of assets within the function | [PE.L2-3.10.2] |
| | k. | More rigorous cybersecurity controls are implemented for higher priority assets | |
| MIL3 | l. | Configuration of and changes to firmware are controlled throughout the asset lifecycle | |
| | m. | Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code | [CM.L2-3.4.8] [CM.L2-3.4.9] [SC.L2-3.13.13] [SI.L2-3.14.2] |

## 4. Implement Software Security as an Element of the Cybersecurity Architecture

| | | |
|---|---|---|
| **MIL1** | No practice at MIL1 | |
| **MIL2** | a. Software developed in-house for deployment on higher priority assets is developed using secure software development practices | [SC.L2-3.13.2] |
| | b. The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices | |
| | c. Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house | [SC.L2-3.13.2] |
| **MIL3** | d. All software developed in-house is developed using secure software development practices | [SC.L2-3.13.2] |
| | e. The selection of all procured software includes consideration of the vendor's secure software development practices | |
| | f. The architecture review process evaluates the security of new and revised applications prior to deployment | [CM.L2-3.4.3] [SC.L2-3.13.2] |
| | g. The authenticity of all software and firmware is validated prior to deployment | |
| | h. Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events | [SC.L2-3.13.2] |

## 5. Implement Data Security as an Element of the Cybersecurity Architecture

| | | | |
|---|---|---|---|
| MIL1 | a. | Sensitive data is protected at rest, at least in an ad hoc manner | |
| MIL2 | b. | All data at rest is protected for selected data categories | [PE.L2-3.10.6] [SC.L2-3.13.16] |
| | c. | All data in transit is protected for selected data categories | [AC.L2-3.1.3] [SC.L2-3.13.8] |
| | d. | Cryptographic controls are implemented for data at rest and data in transit for selected data categories | [AC.L2-3.1.13] [AC.L2-3.1.17] [AC.L2-3.1.19] [IA.L2-3.5.10] [MP.L2-3.8.6] [MP.L2-3.8.9] [SC.L2-3.13.8] [SC.L2-3.13.11] [SC.L2-3.13.16] |
| | e. | Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls | [SC.L2-3.13.10] |
| | f. | Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented | [AC.L2-3.1.3] |
| MIL3 | g. | The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen | [MP.L2-3.8.6] [SC.L2-3.13.16] |
| | h. | The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data | [CM.L2-3.4.5] |

## 6. Management Activities for the ARCHITECTURE domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel |
| | e. | Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked |

## Cybersecurity Program Management (PROGRAM)

*Purpose: Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.*

### Objectives and Practices

### 1. Establish Cybersecurity Program Strategy

| | | |
|---|---|---|
| MIL1 | a. | The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner |
| MIL2 | b. | The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities |
| | c. | The cybersecurity program strategy and priorities are documented and aligned with the organization's mission, strategic objectives, and risk to critical infrastructure |
| | d. | The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities |
| | e. | The cybersecurity program strategy defines the structure and organization of the cybersecurity program |
| | f. | The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program |
| | g. | The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC) |
| MIL3 | h. | The cybersecurity program strategy is updated periodically and according to defined triggers, such as business changes, changes in the operating environment, and changes in the threat profile (THREAT-2e) |

## 2. Establish and Maintain Cybersecurity Program

| | | |
|---|---|---|
| MIL1 | a. | Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner |
| MIL2 | b. | The cybersecurity program is established according to the cybersecurity program strategy |
| | c. | Senior management sponsorship for the cybersecurity program is visible and active |
| | d. | Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies |
| | e. | Responsibility for the cybersecurity program is assigned to a role with sufficient authority |
| | f. | Stakeholders for cybersecurity program management activities are identified and involved |
| MIL3 | g. | Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy |
| | h. | Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes |
| | i. | The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate |
| | j. | The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies |

## 3. Management Activities for the PROGRAM domain

| | | |
|---|---|---|
| MIL1 | No practice at MIL1 | |
| MIL2 | a. | Documented procedures are established, followed, and maintained for activities in the PROGRAM domain |
| | b. | Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain |
| MIL3 | c. | Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain |
| | d. | Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel |
| | e. | Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities |
| | f. | The effectiveness of activities in the PROGRAM domain is evaluated and tracked |

# APPENDIX A: CMMC ASSESSMENT CONSIDERATIONS

This section details considerations for organizations seeking CMMC certification that have:

- performed a C2M2 self-evaluation, or
- may be working towards the completion of a C2M2 self-evaluation.

Levels 1 and 2 CMMC requirements are detailed in this section and are arranged in the same order as the Level 2 *CMMC Assessment Guide* that has been released by the Department of Defense.

# Access Control

## AC.L2-3.1.1

CMMC Short Name: Authorized Access Control

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

NIST SP 800-171 Reference: 3.1.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1b | Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner |
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ARCHITECTURE-3a | Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner |

### Discussion

Largely Implementing or Fully Implementing ACCESS-1b, ACCESS-2a, ACCESS-2c, and ARCHITECTURE-3a will likely provide a capability similar to AC.L2-3.1.1. To satisfy the assessment objectives of AC.L2-3.1.1, an organization should implement a method to identify and approve users, processes acting on behalf of users, and devices that are authorized to access resources, such as files or devices. This capability helps enable an organization to audit the actions of users, processes acting on behalf of authorized users, and devices.

Before access is granted to an information system, an organization should use a defined method to grant authorization. For example, a user needs access to an internal datastore that stores restricted information, and an organization requires the user to request authorization to access the datastore. This can be accomplished with a help desk process that verifies that a user is authorized to access the resource. After a resource owner gives approval, the help desk grants access to the user.

## AC.L2-3.1.2

CMMC Short Name: Transaction & Function Control

Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

NIST SP 800-171 Reference: 3.1.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |

### Discussion

Largely Implementing or Fully Implementing ACCESS-1h, ACCESS-2a, and ACCESS-2c will likely provide a capability similar to AC.L2-3.1.2. Access to such resources as applications and data should be limited to the resources necessary for a user to fulfill job responsibilities. The defined access requirements should be used to limit access to resources, for example, restricting a user to only read access to a shared folder, but giving full write access to a personal folder for storing files.

A small organization may store sensitive customer information in a shared folder and have a policy that restricts users from copying the information to their laptops. Access to the shared folder is restricted, and is granted based on user job role. An access control list is implemented that allows only users from a customer support team to access the information.

## AC.L2-3.1.20

CMMC Short Name: External Connections

Verify and control/limit connections to and use of external information systems.

NIST SP 800-171 Reference: 3.1.20

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2f | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) |

### Discussion

Organizations that have Fully Implemented or Largely Implemented ARCHITECTURE-2f will likely have a capability similar to AC.L2-3.1.20. It is important to note that "external information systems" will be dependent upon the CMMC Assessment Scope. These may be systems that are outside an organization's network, or could be inside an organization's network if a the CMMC Assessment Scope is a limited portion of an organization's network (e.g., enclave, lab).

An organization should first identify and document connections that are made to and from external systems. With the interconnected and collaborative nature of many organizations, this could include connections to partners or vendors. Controls must be implemented that can verify and control these connections. For example, a Virtual Private Network (VPN) can be implemented that requires a vendor to use unique credentials. An organization may also consider implementing policies that define acceptable use of external systems.

## AC.L2-3.1.22

CMMC Short Name: Control Public Information

Control information posted or processed on publicly accessible information systems.

NIST SP 800-171 Reference: 3.1.22

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| WORKFORCE-1e | Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets |

### Discussion

Organizations that have Fully Implemented or Largely Implemented WORKFORCE-1e may have some of the necessary capability to meet the requirements of AC.L2-3.1.22. This CMMC requirement does have specific requirements regarding CUI that organizations should consider in the implementation of these practices.

It is important for organizations to implement policies and procedures regarding the handling of sensitive information, such as CUI. To meet the requirements of this practice, an organization should identify whether these procedures are in place and develop a process to review content that will be made public to ensure it does not contain CUI. An organization should identify individuals responsible for posting information publicly, as well as those responsible for reviewing content and those who have the ability to remove public content if it is discovered that CUI has been posted improperly.

## AC.L2-3.1.3

CMMC Short Name: Control CUI Flow

Control the flow of CUI in accordance with approved authorizations.

NIST SP 800-171 Reference: 3.1.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5c | All data in transit is protected for selected data categories |
| ARCHITECTURE-5f | Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented |

### Discussion

Largely Implementing or Fully Implementing ARCHITECTURE-5c and ARCHITECTURE-5f will likely help an organization implement the requirements needed to meet AC.L2-3.1.3, but an organization must consider CUI-specific requirements. To meet the assessment objectives of AC.L2-3.1.3, an organization must understand how information flows through the network and, more specifically, information classified as CUI. Organizations should consider categorizing their information to help gain a better understanding of storage locations for all CUI and the ways it is transmitted throughout the network or other interconnected networks. An understanding of CUI flow helps an organization build network protections that can control the flow of CUI throughout the network.

An organization has a policy that requires sensitive information, such as CUI, may only be stored, processed, and transmitted by workstations located on a specific network subnet. Network protection devices are configured based on this policy to restrict the flow of data like CUI. Users are trained to follow handling procedures for sensitive data and only transmit the information out of an organization using encrypted email.

## AC.L2-3.1.4

CMMC Short Name: Separation of Duties

Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

NIST SP 800-171 Reference: 3.1.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1a | Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities) |
| ACCESS-2e | Logical access requirements incorporate the principle of separation of duties |
| ACCESS-3f | Physical access requirements incorporate the principle of separation of duties |

### Discussion

Organizations that have Fully Implemented or Largely Implemented ACCESS-1a, ACCESS-2e, and ACCESS-3f will likely have a capability similar to meet the requirements of AC.L2-3.1.4, but should ensure that they have considered and defined job duties assigned to separate individuals. Furthermore, access privileges should be built around separation of duty requirements that ensure that individuals cannot access multiple functions that could result in malevolent activity.

Separate identities for all users helps organizations meet this practice, because it gives them the ability to separate user access by specific system functions or information. For example, it is common to separate the activity of creating a user account and granting privileges to an account.

## AC.L2-3.1.5

CMMC Short Name: Least Privilege

Employ the principle of least privilege, including for specific security functions and privileged accounts.

NIST SP 800-171 Reference: 3.1.5

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2d | Logical access requirements incorporate the principle of least privilege |

### Discussion

Fully Implementing or Largely Implementing ACCESS-2d may provide a capability similar to the requirements of AC.L2-3.1.5. An organization should carefully consider whether least privilege is being enforced for privileged accounts, particularly those that can access security functions.

Organizations may consider restricting the use of privileged accounts to certain roles, particularly roles with an operational need to perform security functions. For example, a network administrator may be responsible for managing firewall rules. An organization can restrict access to the firewall configuration to a dedicated privileged account separate from the network administrator's standard user account.

## AC.L2-3.1.6

CMMC Short Name: Non-Privileged Account Use

Use non-privileged accounts or roles when accessing nonsecurity functions.

NIST SP 800-171 Reference: 3.1.6

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1g | The use of privileged credentials is limited to processes for which they are required |

### Discussion

An organization that has Fully Implemented or Largely Implemented ACCES-1g will likely have a capability similar to AC.L2-3.1.6. To achieve this practice, an organization should ensure that it has considered and defined the functions that only privileged accounts should complete, and those that standard accounts should complete. All users should be provided with a standard access account for nonsecurity functions. Some users (e.g., system administrators, IT staff) may have a job responsibility that requires privileged access. Such responsibilities include changing system configuration settings, or adding an application to an allowlist. Users with these responsibilities should have a separate account specifically for this privileged access use.

Policies, procedures, and training for users who are granted privileged access should include restrictions on the use of privileged accounts for job responsibilities that do not require such accounts. An organization should identify activities that require privileged access, such as changing detection rules for an intrusion detection system (IDS). A network security engineer who is responsible for maintaining the detection rules will be issued a separate administrative account for use when updating the detection rules, but not for use on nonsecurity functions, such as checking email messages or reviewing documentation.

## AC.L2-3.1.7

CMMC Short Name: Privileged Functions

Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.

NIST SP 800-171 Reference: 3.1.7

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ACCESS-2g | Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring |
| SITUATION-1a | Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner |
| SITUATION-1c | Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective |
| SITUATION-1d | Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems) |

### Discussion

An organization that has Fully Implemented or Largely Implemented ACCESS-1h, ACCESS-2c, ACCESS-2g, SITUATION-1a, SITUATION-1c, and SITUATION-1d will likely have a capability similar to AC.L2-3.1.7. Achievement of this practice requires that an organization defines privileged functions; clearly distinguishes between privileged and non-privileged accounts; limits execution of privileged functions; and logs execution of privileged functions.

An organization should identify and document privileged functions to enable the building of security controls around these functions. This will limit execution by standard users and implement logging to identify the execution of the privileged functions. If a job role requires a user to perform privileged functions, additional permissions should be granted to allow the user to perform those functions. This can be achieved by granting the additional permissions to a separate administrative user account. Regardless of the type of account or permissions granted to an account, the execution of privileged functions should be logged. Logging all privileged functions enables the identification of non-privileged users who attempt to

execute privileged functions, and of incorrect allocation of permissions that can result in misuse of privileged functions.

## AC.L2-3.1.8

CMMC Short Name: Unsuccessful Logon Attempts

Limit unsuccessful logon attempts.

NIST SP 800-171 Reference: 3.1.8

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3a | Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner |

### Discussion

Organizations that have Fully Implemented or Largely Implemented ARCHITECTURE-3a will likely have a capability similar to AC.L2-3.1.8. Controls that limit unsuccessful logon attempts would likely be included in the asset configuration requirements derived from a cybersecurity architecture.

Limiting unsuccessful logon attempts helps mitigate attacks, such as a brute force attack on a user account. Authentication points where this type of attack could be executed should be identified and documented. These may include operating systems, software applications, or web-based applications. Methods to limit unsuccessful logon attempts should be identified and implemented at all authentication points. The methods may be built in to software, similar to setting an account lockout threshold policy setting in an operating system.

## AC.L2-3.1.9

CMMC Short Name: Privacy & Security Notices

Provide privacy and security notices consistent with applicable CUI rules.

NIST SP 800-171 Reference: 3.1.9

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice. This CMMC requirement is focused specifically on notifying users of their legal requirements when using a system that stores, transmits, or processes CUI.

Organizations may have an existing system use notification that informs users of acceptable use and system use monitoring. A similar function can be implemented that also identifies CUI-specific requirements and requires a user to agree to them prior to using the system. This may also be implemented at the application level in addition to or in place of a system use notification. If implementing a system notification is not feasible, an organization can implement signage that provides a similar notification.

## AC.L2-3.1.10

CMMC Short Name: 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 Reference: 3.1.10

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice. Implementation of this practice helps mitigate misuse of a system by an unauthorized user if a system is left unlocked while a user is away.

Most operating systems have built in functions to configure a system to lock after a period of inactivity, then display a lock screen that obscures the information on the screen. An organization should first, define a period of inactivity that triggers the operating system to lock a session, then implement this threshold in the configuration setting of all in-scope assets. In addition, a lock screen that does not allow the information on the screen to be viewed without unlocking the system should be included in the configuration.

## AC.L2-3.1.11

CMMC Short Name: Session Termination

Terminate (automatically) a user session after a defined condition.

NIST SP 800-171 Reference: 3.1.11

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3e | Secure configurations are established and maintained as part of the asset deployment process where feasible |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3e may provide some of the same capability as AC.L2-3.1.11, but organizations should review carefully the specific requirements detailed in the assessment objectives. This CMMC requirement requires user-initiated logical sessions to be terminated automatically if defined conditions are met. The conditions can be configured based on such criteria as a period of time or other defined conditions, for example, accessing application functionality that has not been granted to a user.

An organization can use an application such as a remote desktop client to configure OT assets from the enterprise network. The client should be configured so that a user session terminates after a defined period of time to prevent misuse of the session by an attacker. Monitoring user activity can also trigger termination of a session, for example, accessing information in a database if a user does not have sufficient read permissions.

## AC.L2-3.1.12

CMMC Short Name: Control Remote Access

Monitor and control remote access sessions.

NIST SP 800-171 Reference: 3.1.12

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ARCHITECTURE-2c | Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices) |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1h, ACCESS-2c, and ARCHITECTURE-2c will likely help an organization meet AC.L2-3.1.12, but additional review of the specific requirements detailed in the assessment objectives is recommended. Although this practice requires the control and monitoring of remote access, documented policy on remote access is also important.

Organizations should consider carefully the risk that implementing remote access can introduce, particularly for those who handle CUI. Remote access that meets organizational thresholds should be expressed in policy, which can be used to implement a solution that meets the stated requirements. The policy should include permitted remote access methods, along with requirements for controlling and monitoring remote access. For example, an organization states that systems should be configured to use only a specific remote access solution, and that remote access should be monitored in conjunction with other logs on a continuous basis.

## AC.L2-3.1.13

CMMC Short Name: Remote Access Confidentiality

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

NIST SP 800-171 Reference: 3.1.13

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2c | Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices) |
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2c and ARCHITECTURE-5d will likely provide the same capability as described in AC.L2-3.1.13. However, organizations should consider carefully if their implementation of remote access meets the specific requirements of this CMMC requirement.

If not properly secured, remote access can serve as a threat vector for attackers. Encrypting remote network access provides protection for information transmitted between two locations, such as between home and corporate networks or between a corporate network and a cloud service. This functionality is common in remote access solutions, but extra consideration should be given when selecting and implementing a solution to protect CUI. To meet this CMMC requirement, the remote access solution must use FIPS-validated cryptography. The cryptographic module to implement the algorithm must be validated under FIPS 140. The NIST Cryptographic Module Validation Program (CMVP) website lists validated modules.

## AC.L2-3.1.14

CMMC Short Name: Remote Access Routing

Route remote access via managed access control points.

NIST SP 800-171 Reference: 3.1.14

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2c | Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2j will likely provide the same capability as described in AC.L2-3.1.14, but organizations should consider carefully if their implementation of remote access meets the specific requirements of this CMMC requirement.

One way that organizations can employ to reduce the risk of remote access solutions is to reduce the number of points from which remote access can enter the internal network. This provides greater control over remote access sessions and allows for better monitoring. Organizations that have implemented this capability should ensure that they have identified and documented managed remote access control points. Monitoring of network traffic can help an organization identify if rogue remote access sessions are subverting the managed control points.

## AC.L2-3.1.15

CMMC Short Name: Privileged Remote Access

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

NIST SP 800-171 Reference: 3.1.15

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ACCESS-2f | Logical access requests are reviewed and approved by the asset owner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1h, ACCESS-2c, and ACCESS-2f will likely provide a capability similar to the requirements of this AC.L2-3.1.15. When implementing a remote access solution, additional consideration should be given to remote access that allows the execution of privileged commands or the access of security-relevant information.

An organization may grant some users permissions necessary to execute privileged commands. For example, a system administrator may have the permission to change logging configuration settings on organizational systems. Organizations should carefully consider if these users should be permitted to execute these commands remotely. The privileged commands and security-relevant information that users are permitted to access should be documented and used in access authorizations.

## AC.L2-3.1.16

CMMC Short Name: Wireless Access Authorization

Authorize wireless access prior to allowing such connections.

NIST SP 800-171 Reference: 3.1.16

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-1a | IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ARCHITECTURE-2k | Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control (NAC)) |

### Discussion

Fully Implemented or Largely Implemented ASSET-1a, ACCESS-2c, and ARCHITECTURE-2k will likely have a capability similar to AC.L2-3.1.16. To meet this CMMC requirement, an organization should have an inventory of all authorized wireless access points, and should define and enforce requirements for devices establishing wireless connections.

Many organizations have a business need to implement wireless networking to enable communication with a variety of devices, such as laptops, internet of things (IoT) devices, remote sensors, and facility environmental control systems. When building or updating an asset inventory, organizations should include wireless networking infrastructure, such as wireless access points. In addition, an organization should define requirements that must be met prior to authorizing a wireless connection, such as device configuration requirements. Wireless access should require user authentication similar to the requirements in place for wired connections.

## AC.L2-3.1.17

CMMC Short Name: Wireless Access Protection

Protect wireless access using authentication and encryption.

NIST SP 800-171 Reference: 3.1.17

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implemented or Largely Implemented both ACCESS-2a and ARCHITECUTRE-5d will likely meet the requirements for AC.L2-3.1.17. Organizations should ensure that FIPS-validated cryptography is used for encrypting wireless communications, because it is required when CUI is transmitted or stored outside the protected environment of a covered contractor information system.

Implementation of this CMMC requirement may vary depending on the size of an organization. Authentication may be by a pre-shared key through an authentication scheme like WPA2, or through domain credentials for solutions that interface with a RADIUS server. Selection criteria for wireless devices and supporting network infrastructure should include the ability to use FIPS-validated encryption modules for encryption. The NIST Cryptographic Module Validation Program (CMVP) website lists modules that have been validated.

## AC.L2-3.1.18

CMMC Short Name: Mobile Device Connection

Control connection of mobile devices.

NIST SP 800-171 Reference: 3.1.18

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |
| SITUATION-1a | Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner |
| SITUATION-2g | More rigorous monitoring is performed for higher priority assets |
| ARCHITECTURE-2k | Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control (NAC)) |

### Discussion

Fully Implementing or Largely Implementing ACCESS-2a, SITUATION-1a, SITUATION-2g, and ARCHITECTURE-2k will likely provide a capability similar to AC.L2-3.1.18. Additional consideration should be given to the CUI requirements of this CMMC requirement.

Organizations should balance risk and business needs when permitting CUI or other sensitive information to be accessed and stored on mobile devices. These devices must be identified according to defined procedures to ensure that an organization is able to monitor and log connections adequately from the devices. The devices should be permitted to connect to an organization's network only after being approved and authorized. A mobile device management (MDM) solution can help an organization identify, manage, and monitor the devices.

## AC.L2-3.1.19

CMMC Short Name: Encrypt CUI on Mobile

Encrypt CUI on mobile devices and mobile computing platforms.

NIST SP 800-171 Reference: 3.1.19

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5d may provide a capability similar to AC.L2-3.1.19. This CMMC requirement has CUI-specific requirements that require additional consideration by an organization.

Mobile devices that are permitted to access CUI, such as smartphones, introduce unique challenges because they can be lost or stolen more easily than other organizational assets. Implementing encryption to prevent disclosure of CUI or other sensitive information helps mitigate this risk. Like other CMMC requirements that require the use of cryptography, this practice requires FIPS-validated cryptography. Organizations can consider the implementation of a mobile device management (MDM) solution that enforces this functionality and includes FIPS-validated cryptography.

## AC.L2-3.1.21

CMMC Short Name: Portable Storage Use

Limit use of portable storage devices on external systems.

NIST SP 800-171 Reference: 3.1.21

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3g | The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3g may provide a capability similar to AC.L2-3.1.21, but this practice has CUI-specific requirements that organizations need to consider.

Organizations that handle CUI should consider if there is a valid business need for removeable media to be used on systems within the CMMC Assessment Scope. Implementation of this CMMC requirement varies based on the scope and size of an organization. For example, a small organization that has an enterprise-level scope may determine it is sufficient to designate and label specific removeable media to store CUI and limit administratively the use of these devices outside an organization. A larger organization may take a different approach, including implementing technical controls that allow only authorized removeable media to be used on systems within the CMMC Assessment Scope.

# Awareness and Training

## AT.L2-3.2.1

CMMC Short Name: 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 Reference: 3.2.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| WORKFORCE-1e | Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets |
| WORKFORCE-2d | Cybersecurity awareness activities are conducted periodically |
| WORKFORCE-2e | Cybersecurity awareness activities are tailored to job role |

### Discussion

Fully Implementing or Largely Implementing WORKFORCE-1e, WORKFORCE-2d, and WORKFORCE-2e may meet AT.L2-3.2.1 requirements. However, organizations should consider the CUI-specific requirements of this CMMC requirement.

Organizations should ensure that individuals trusted with sensitive information, such as CUI, are made aware of their responsibilities to prevent the disclosure of such information. Similarly, individuals who have privileged access to systems and resources should be made aware of their increased responsibility and of the implications if the access is misused. This can be achieved through awareness training and regular communications. Employee responsibility for information and data security should be documented in policies. An organization should make employees aware of the requirements during awareness activities and in an ongoing manner, such as through logon banners.

## AT.L2-3.2.2

CMMC Short Name: Role-Based Training

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

NIST SP 800-171 Reference: 3.2.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| WORKFORCE-4a | Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner |
| WORKFORCE-4c | Identified cybersecurity knowledge, skill, and ability gaps are addressed through training, recruiting, and retention efforts |
| WORKFORCE-4d | Cybersecurity training is provided as a prerequisite to granting access to assets that are important to the delivery of the function |

### Discussion

Fully Implementing or Largely Implementing WORKFORCE-4a, WORKFORCE-4c, and WORKFORCE-4d will likely provide a capability similar to AT.L2-3.2.2.

Staff with cybersecurity duties have unique responsibilities. Organizations should document the roles and responsibilities necessary to properly secure sensitive information. Assigning cybersecurity-related duties, -roles, and -responsibilities ensures that there are no gaps between necessary requirements to secure information and their actual implementation. In addition, it is essential that an organization evaluates continually if staff members responsible for cybersecurity-related duties has the necessary training to carry out their assigned responsibilities. Organizations can consider building training plans for roles to ensure that staff are consistently building their knowledge and skills to support the cybersecurity program.

## AT.L2-3.2.3

CMMC Short Name: Insider Threat Awareness

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

NIST SP 800-171 Reference: 3.2.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| WORKFORCE-2c | Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e) |

### Discussion

Fully Implementing or Largely Implementing WORKFORCE-2c may provide a capability similar to AT.L2-3.2.2, but organizations should ensure that the specific insider-threat-focused requirements are covered by awareness activities.

Insider threats pose a unique risk to organizations because they stem from trusted individuals. These include both actions that cause intentional harm and unintentional actions that cause harm to an organization, such as an employee who is socially engineered. Organizations should consult literature focused on indicators that can be used to identify insider threats, and build awareness training around these indicators. Early identification of the threats reduces the potential impact to an organization.

# Audit and Accountability

## AU.L2-3.3.1

CMMC Short Name: 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 Reference: 3.3.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| RESPONSE-1c | Cybersecurity events are documented based on the established criteria |
| SITUATION-1a | Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner |
| SITUATION-1c | Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective |
| SITUATION-1d | Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems) |

### Discussion

Fully Implementing or Largely Implementing RESPONSE-1c, SITUATION-1a, SITUATION-1c, and SITUATION-1d will likely provide a capability similar to AU.L2-3.3.1. Logging is commonly enabled on devices, and logs are rarely reviewed until something breaks. This may seem sufficient with respect to the health of physical devices, but such an approach does not increase an organization's cyber resiliency.

Simply enabling logging on devices, systems, and user accounts is not sufficient to protect operating environments. It does not meet the intent of this practice, and will likely fail a third party audit. Irrespective of any compliance requirements, logging and monitoring are intended to provide an early indication of suspicious activity, provide information to support a forensics investigation should an incident occur, and provide an audit trail of changes and access to systems.

Key to determining the adequacy of current SITUATION practice implementation with respect to CMMC are:

- An organization has defined logging and review requirements.
- Assets are configured to produce logs consistent with policy.
- A log retention policy is established and enforced.

Although not called out specifically, a SIEM solution is a cost effective way to collect the huge volumes of log data created; correlate events across multiple platforms; protect logs from tampering; and help meet retention requirements. They are especially valuable in triggering alerts about suspicious behavior and any subsequent forensic investigation. Cost is a function of the amount of data collected over a given period (typically monthly) and the retention period and type.

Organizationally, there is a lot of leeway in what is captured and reviewed, provided it provides enough detail to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Even if CUI is never processed, logs from Security Protection Assets are critical to meeting the intent and requirements of this requirement. Specialized Assets and Contractor Risk Managed Assets may not be assessed in the same way as other assets, but they still need to be protected and monitored. See the CMMC scoping guides for details.

## AU.L2-3.3.2

CMMC Short Name: 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 Reference: 3.3.2

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| SITUATION-1c | Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective |
| SITUATION-1d | Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems) |

### Discussion

Fully Implementing or Largely Implementing SITUATION-1c and SITUATION-1d may provide a capability similar to AU.L2-3.3.2, but organizations should ensure that the CMMC-specific requirements are reviewed. In the context of this CMMC requirement, "established and maintained" should include confirmation that audit records contain the content defined in logging requirements. A solid implementation of user controls and account access in other areas helps make this practice achievable.

In addition to not sharing user accounts, an organization should capture as much information about the user performing a transaction on a system. This includes such data as user IDs, source and destination addresses, and time stamps. An organization should use multiple data points, as well. User authentication data coupled with MFA logs increase the likelihood that a specific user performed the audited action. In addition, it is important to ensure that these data points are identified in your system auditing policy.

## AU.L2-3.3.3

CMMC Short Name: Event Review

Review and update logged events.

NIST SP 800-171 Reference: 3.3.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| SITUATION-1c | Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective |
| SITUATION-1d | Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems) |
| SITUATION-2c | Monitoring and analysis requirements are established and maintained for the function and address timely review of event data |

### Discussion

Fully Implementing or Largely Implementing SITUATION-1c, SITUATION-1d, and SITUATION-2c will likely provide the same capability as AU.L2-3.3.3. This practice is focused on the configuration of the auditing system, not the review of the audit records produced by the selected events. Organizations should ensure that their audit policies are up to date, are periodically reviewed, and reflect changes in their infrastructure as well as in the evolving threat landscape. In particular, they should ensure that an organization's retention policies reflect the fact that incidents often go undetected for weeks or months, and that longer term storage of audit logs may be needed to provide the information to support an investigation.

Additionally, organizations should ensure that the data collected is at the proper level and detail, and that the logs from the correct systems are being maintained. Logging configurations should be updated when there is a change to security assets and when major system changes occur. As a reminder when using cloud service providers (CSP), the default logging and retention may be for as short as seven days and capture only the barest minimum of data.

## AU.L2-3.3.4

CMMC Short Name: Audit Failure Alerting

Alert in the event of an audit logging process failure.

NIST SP 800-171 Reference: 3.3.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| SITUATION-2e | Alarms and alerts are configured and maintained to support the identification of cybersecurity events |

### Discussion

Fully Implementing or Largely Implementing SITUATION-2e may provide some of the capability of AU.L2-3.3.4, but organizations should review the assessment requirements of this CMMC requirement to determine if their implementation meets these requirements. Audit logging process failures include software and hardware errors, failures in the audit record capturing mechanisms, and audit record storage capacity being reached or exceeded. This requirement applies to each audit record data storage repository (i.e., distinct system component where audit records are stored), the total audit record storage capacity of organizations (i.e., all audit record data storage repositories combined), or both.

Audit logging keeps track of activities occurring on the network, servers, user workstations, and other components of the overall system. These logs must always be available and functional. The company's designated security personnel (e.g., system administrator and security officer) need to be aware when the audit log process fails or becomes unavailable. Notifications (e.g., email, Short Message Service (SMS)) should be sent to the company's designated security personnel for immediate and appropriate action. If security personnel are unaware of the audit logging process failure, then they will be unaware of any suspicious activity occurring at that time. Response to an audit logging process failure should account for the extent of the failure (e.g., a single component's audit logging versus failure of the centralized logging solution), the risks involved in this loss of audit logging, and other factors (e.g., the possibility that an adversary could have caused the audit logging process failure).

## AU.L2-3.3.5

CMMC Short Name: 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 Reference: 3.3.5

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| SITUATION-2a | Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner |
| SITUATION-2b | Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner |
| SITUATION-2c | Monitoring and analysis requirements are established and maintained for the function and address timely review of event data |
| SITUATION-3d | Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders |
| SITUATION-3f | A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function |

### Discussion

Fully Implementing or Largely Implementing SITUATION-2a, SITUATION-2b, SITUATION-2c, SITUATION-3d, and SITUATION-3f will likely provide the same capability as AU.L2-3.3.5. Smaller organizations may be able to perform these practices manually with well-defined and -managed procedures. Mid-sized and large organizations will likely use some type of automated system that correlates log information from across the enterprise. SITUATION-3d and SITUATION-3e cannot be implemented realistically without the use of an automated tool (i.e., a SIEM).

When preparing for a CMMC assessment, some material developed for RESPONSE-1 and RESPONSE-2 may also be applicable.

An automated SIEM (preferably managed) provides a far greater level of accuracy in correlating events, and in identifying possible incidents, at a much lower cost. Additionally, the practice is easy for an auditor to validate when an organization employs an automated tool.

## AU.L2-3.3.6

CMMC Short Name: Reduction & Reporting

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

NIST SP 800-171 Reference: 3.3.6

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| SITUATION-3f | A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function |

### Discussion

Fully Implementing or Largely Implementing SITUATION-3f may provide the capability of AU.L2-3.3.6, but the specific requirements of this CMMC requirement should be reviewed. The volume of data makes raw audit log data difficult to review, analyze, and report. Audit record reduction is an automated process that interprets raw audit log data and extracts meaningful and relevant information without altering the original logs.

While not identical to SITUATION-3e, the tools and processes implemented are likely applicable to this CMMC requirement. The objective of both practices is to distill the huge amount of data captured into meaningful information; provide an alert capability based on patterns and trends in the data; and, for CMMC, support forensic investigations. The tools already deployed can likely be configured to do more than capture and aggregate log data, especially if it is a true SIEM solution. Many of these platforms can ingest threat information and use it as a comparison to aggregated data in an organization's systems. When configuring them, organizations should look at data retention settings. In many cases, possible intrusions and compromises are not detected for weeks or even months. Organizations should ensure that the retention period is set to a long enough period to support meaningful forensics investigations.

## AU.L2-3.3.7

CMMC Short Name: 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 Reference: 3.3.7

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice. Organizations should consider how the requirements of this practice relate to their current cybersecurity architecture. Each system must synchronize its time with a central time server to ensure that all systems are recording audit logs using the same time source. Reviewing audit logs from multiple systems can be a difficult task if time is not synchronized. In order to communicate reliably, devices must have synchronized clocks. Organizations should be aware of the settings used by default, and ensure that all devices use a common standard.

## AU.L2-3.3.8

CMMC Short Name: Audit Protection

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

NIST SP 800-171 Reference: 3.3.8

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2g | Logical access that poses higher risk to the function receives additional scrutiny and monitoring |

### Discussion

Fully Implementing or Largely Implementing ACCESS-2g will likely provide some of the capability of AU.L2-3.3.8, but the specific requirements of this CMMC requirement should be reviewed. Access to audit logging tools and audit information will likely be considered higher risk to the function, but organizations should confirm if this is reflected in their logical access policies.

Assuming that an organization has deployed an automated tool to capture, analyze, aggregate, and store its audit logs, most of the requirement in CMMC has probably been met. An organization's tool should pull the logs from all sources, then store them in a way that prevents modification. Additionally, the list of users who can access them for read-only purposes should be limited and tightly controlled. The original system logs should be similarly protected, but the tool can serve as the definitive archive if properly configured.

## AU.L2-3.3.9

CMMC Short Name: Audit Management

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

NIST SP 800-171 Reference: 3.3.9

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ACCESS-2f | Logical access requests are reviewed and approved by the asset owner |
| ACCESS-2g | Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1h, ACCESS-2c, ACCESS-2f, and ACCESS-2g will likely provide capability similar to AU.L2-3.3.9, but additional review of the CMMC requirements may be required. The key to this practice is a strict limit of which privileged users can access and configure audit logs and audit settings. Related to how an organization separates duties, those responsible for implementing changes should not be the same users responsible for reviewing the audit records that capture those changes. Ensure that multiple methods are in place to grant access and that audit logs cannot be altered or deleted.

As previously discussed, the tools that have deployed to capture and analyze log information can be a great resource for protecting audit information and server as another level of separation to restrict access to a subset of users.

# Configuration Management

## CM.L2-3.4.1

CMMC Short Name: 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 Reference: 3.4.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-1f | The IT and OT asset inventory is complete (the inventory includes all assets within the function) |
| ASSET-2f | The information asset inventory is complete (the inventory includes all assets within the function) |
| ASSET-3a | Configuration baselines are established, at least in an ad hoc manner |
| ASSET-3e | Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles |

### Discussion

Fully Implementing or Largely Implementing ASSET-1f, ASSET-2f, ASSET-3a, and ASSET-3e will likely provide a capability similar to CM.L2-3.4.1. An accurate asset inventory and the implementation of secure configuration baselines are enabling functions for many other cybersecurity activities, such as vulnerability management, incident identification, and host monitoring.

Organizations may consider procedures for building and maintaining an asset inventory and employing tools that perform automated device discovery. Similarly, procedures that define how configuration baselines should be built and maintained may improve the consistency of systems deployed throughout an organization. Organizations may consider defining additional requirements, such as approved sources for operating system or application patches.

## CM.L2-3.4.2

CMMC Short Name: Security Configuration Enforcement

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

NIST SP 800-171 Reference: 3.4.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-3c | Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f) |
| ASSET-3e | Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles |
| ARCHITECTURE-1c | A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization |
| ARCHITECTURE-1i | Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events |
| ARCHITECTURE-3e | Secure configurations are established and maintained as part of the asset deployment process where feasible |
| ARCHITECTURE-3f | Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls) |

### Discussion

Fully Implementing or Largely Implementing ASSET-3c, ASSET-3e, ARCHITECTURE-1c, ARCHITECTURE-1h, ARCHITECTURE-3e, and ARCHITECTURE-3f will likely provide a capability similar to CM.L2-3.4.2. In the development of configuration baselines or other situations when an asset is put into service, organizations should consider whether configuration settings are in alignment with organizational security requirements.

Most assets require additional configuration before deployment to properly function in an organization’s unique environment. Organizations should also consider if asset configurations meet an organization’s security policies, compliance requirements, or other safety and reliability requirements. In some instances, the default configuration of an asset can introduce additional risk to an organization through a vulnerability like an open port that a threat actor can leverage for an initial compromise of the network.

## CM.L2-3.4.3

CMMC Short Name: System Change Management

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

NIST SP 800-171 Reference: 3.4.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ASSET-4a | Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner |
| ASSET-4b | Changes to assets are documented, at least in an ad hoc manner |
| ASSET-4g | Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement) |
| ASSET-4i | Change logs include information about modifications that impact the cybersecurity requirements of assets |
| ARCHITECTURE-4f | The architecture review process evaluates the security of new and revised applications prior to deployment |

### Discussion

Fully Implementing or Largely Implementing ASSET-4a, ASSET-4b, ASSET-4g, ASSET-4i, and ARCHITECTURE-4f will likely provide a capability similar to CM.L2-3.4.3. A defined process to manage changes enables an organization to identify more efficiently a change that has had an impact on operations or has introduced a vulnerability.

A core component of configuration management is a documented process that includes a method to submit and track change requests. This method will likely include a workflow that gives the requestor visibility into the status of the request as it is reviewed by appropriate parties, and justification for approving or rejecting a change request. In addition, this process should include a requirement for the individual(s) performing approved changes to log the actions taken to implement the change.

## CM.L2-3.4.4

CMMC Short Name: Security Impact Analysis

Analyze the security impact of changes prior to implementation.

NIST SP 800-171 Reference: 3.4.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ASSET-4h | Changes to assets are tested for cybersecurity impact prior to being deployed |

### Discussion

Fully Implementing or Largely Implementing ASSET-4h will likely provide a capability similar to CM.L2-3.4.4, but the scope of assets within this practice should be reviewed. Changes should be tested prior to implementation for impact on operations. Organizations should also consider how a change could impact the security of an asset, a system, or operating environment.

Prior to implementing a change in a production environment, it is important to consider how it could impact operations and security. Many organizations plan carefully the implementation of changes around scheduled downtime to prevent unintended impacts to production as the result of a change. Changes should be thoroughly tested to identify potential security issues that a change may introduce into the environment. Identification of the issues prior to implementation will mitigate the chance of costly downtime to address the issue.

## CM.L2-3.4.5

CMMC Short Name: Access Restrictions for Change

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

NIST SP 800-171 Reference: 3.4.5

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-4e | Changes and updates are implemented in a secure manner |
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| ACCESS-3d | Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access) |
| ARCHITECTURE-5h | The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data |

### Discussion

Fully Implementing or Largely Implementing ASSET-4e, ACCESS-2a, ACCESS-2c, ACCESS-3a, ACCESS-3d, and ARCHITECTURE-5h will likely provide a capability similar to CM.L2-3.4.5. Controls to prevent unauthorized users from making changes to assets build upon other configuration management practices to ensure that configurations can be maintained within organizational requirements.

Organizations should consider the logical and physical requirements to be met to reduce the likelihood of changes being performed by an unauthorized individual. These requirements may be defined and documented in an access control policy approved by appropriate organizational stakeholders. The policy could be used to develop and implement controls that enforce access restrictions. The controls can include logical access controls, for example, restricting system maintenance to specific dedicated accounts, or physical access controls, such as limited access to the configuration of an asset to a physical management port.

## CM.L2-3.4.6

CMMC Short Name: Least Functionality

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

NIST SP 800-171 Reference: 3.4.6

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3d | The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3d will likely provide the same capability as CM.L2-3.4.6. In addition to CM.L2-3.4.2, which requires secure configurations, organizations should consider whether assets are being configured to provide the least functionality necessary.

It is important for organizations to review carefully configuration settings or functions that are enabled by default, and determine the settings or functions that are not necessary to support operations. For example, an operating system may have a built-in file-sharing protocol or scripting utility that is not needed to meet operational requirements. Organizations should define the system capabilities necessary to meet operational requirements, then disable capabilities that do not meet the defined requirements.

## CM.L2-3.4.7

CMMC Short Name: Nonessential Functionality

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

NIST SP 800-171 Reference: 3.4.7

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3d | The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3d will likely provide the same capability as CM.L2-3.4.7. In addition to CM.L2-3.4.2, which requires secure configurations, organizations should consider whether assets are being configured to provide only necessary functionality.

It is common for many assets to have a default configuration that is designed for ease of implementation rather than for security. Nonessential functionality could introduce unintended vulnerabilities into the operating environment. Organizations should consider defining the programs, functions, ports, protocols, and services that are necessary to meet operational requirements and the assets configured to meet these requirements. Various methods can be used to examine an asset to ensure that it meets defined requirements, such as utilities built into the operating system or the running of a port scan to find functionality that could be disabled to reduce the attack surface of the asset. Failure to harden assets may result in a vulnerable asset that could be leveraged by a threat actor.

## CM.L2-3.4.8

CMMC Short Name: 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 Reference: 3.4.8

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3d | The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced |
| ARCHITECTURE-3m | Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3d and ARCHITECTURE-3m will likely provide the same capability as CM.L2-3.4.8. This practice builds upon the principle of least functionality (CM.L2-3.4.6) and limiting functionality (CM.L2-3.4.7) by using allowlisting and blocklisting to enforce restrictions on unauthorized software.

It is important for organizations to consider the software necessary to meet operational requirements. Furthermore, the implementation of allowlisting can be used to enforce execution of software to only software that has been authorized by an organization, or blocklisting to restrict the execution of prohibited software. Depending on the approach selected, a policy should be developed that describes software that is authorized or denied for use within the operational environment. Controls should be designed and implemented to enforce the documented allowlisting or blocklisting policy.

## CM.L2-3.4.9

CMMC Short Name: User-Installed Software

Control and monitor user-installed software.

NIST SP 800-171 Reference: 3.4.9

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ASSET-3c | Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f) |
| ASSET-3e | Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles |
| ARCHITECTURE-3d | The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced |
| ARCHITECTURE-3m | Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code |

### Discussion

Fully Implementing or Largely Implementing ASSET-3c, ASSET-3e, ARCHITECTURE-3d, and ARCHITECTURE-3m will likely provide a capability similar to CM.L2-3.4.9. Organizations may consider allowing users to install software, but should have measures in place to control and monitor this activity.

Depending on various factors, such as asset reliability requirements, operational requirements, and compliance requirements, organizations should consider restrictions on user-installed software. Although users may have a business need for installing software that is not included in standard baselines, additional software may introduce vulnerabilities into the operating environment. Organizations should establish a policy that documents restrictions on software installation by users and implement controls that enforce this policy. Additional monitoring, such as through operating system logging, should be implemented to detect installation that violates policy.

# Identification and Authorization

## IA.L2-3.5.1

CMMC Short Name: Identification

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

NIST SP 800-171 Reference: 3.5.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1a | Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities) |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1a will likely provide a capability similar to IA.L2-3.5.1. To meet CMMC IA requirements, organizations may need to tighten current identity-related practices.

Access to most systems requires a unique identifier; in general, sharing is not allowed unless required for operational requirements. Management of users, devices, and processes would likely require an implementation that is more mature than this ad hoc C2M2 practice. Organizations should consider policies and procedures that define the creation of accurate, maintained lists of what is allowed to access the organization's assets. In addition, codifying these requirements in an IA policy ensures that users are aware that their actions are traceable to individual users and devices.

## IA.L2-3.5.2

CMMC Short Name: Authentication

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

NIST SP 800-171 Reference: 3.5.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1b | Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner |
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1b and ACCESS-2a will likely provide the same capability as IA.L2-3.5.2. Like Identification, Authentication is not ad hoc in the CMMC framework; organizations should review whether the potential artifacts that an assessor may examines are in place and maintained.

Organizations should consider documenting how systems are accessed and who is responsible for tracking credentials, as well as have a policy in place to revoke credentials when a device is decommissioned, or a user leaves an organization. In addition, authentication documentation and policy may include best practice requirements such as password complexity and password reuse.

## IA.L2-3.5.3

CMMC Short Name: 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 Reference: 3.5.3

DoD 800-171 Assessment Methodology Point Value: 3 – MFA is implemented for only remote and privileged users

5 – MFA not implemented for any users

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1h will likely provide a capability similar to IA.L2-3.5.3. Another way to understand this practice is to consider the single scenario when MFA is NOT required:

- having local access (i.e., sitting at the keyboard of your laptop),
- logging into it with a non-privileged account (an account that is not local admin), and
- not connecting to an organization's network.

This CMMC requirement requires MFA in all other instances.

As a best practice, organizations should consider MFA on all devices and accounts where it can be enabled and enforced. In some instances, it is not feasible to implement MFA, such as with legacy devices or with OT devices that do not have the capability. When MFA cannot be enabled, organizations should consider implementing compensating controls to meet an organization's cybersecurity requirements. Multifactor authentication is not required for access to mobile devices such as smartphones or tablets. These devices are not considered network devices or information systems.

## IA.L2-3.5.4

CMMC Short Name: Replay-Resistant Authentication

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

NIST SP 800-171 Reference: 3.5.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice, however, this functionality is typically found in all commercial products. Ensure that your policies require it, and verify that applications developed and devices employ replay-resistant authentication mechanisms.

Replay-resistant authentication is important because it ensures that, even if network traffic is intercepted by an attacker, the attacker cannot use the captured data for authentication at a later time. For example, the Kerberos authentication protocol operates on tickets that must be requested by a subject to access a resource. The tickets are encrypted before transmission and have timestamps to prevent reuse at a later time.

## IA.L2-3.5.5

CMMC Short Name: Identifier Reuse

Prevent reuse of identifiers for a defined period.

NIST SP 800-171 Reference: 3.5.5

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice. Organizations should consider how policies and procedures permit them to meet the assessment objectives of this CMMC requirement.

Ensure that an organization's policies specify:

- a period when identifiers are not reused, and how to implement this
- how identifiers are retired (i.e., when an employee leaves an organization).

## IA.L2-3.5.6

CMMC Short Name: Identifier Handling

Disable identifiers after a defined period of inactivity.

NIST SP 800-171 Reference: 3.5.6

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1f | Identities are deprovisioned within organization-defined time thresholds when no longer required |
| ACCESS-1j | Identities are disabled after a defined period of inactivity, where feasible |
| ACCESS-2b | Logical access privileges are revoked when no longer needed, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1f, ACCESS-1j, and ACCESS-2b will likely provide a capability similar to IA.L2-3.5.6. Both C2M2 and CMMC require organizations to consider and document these requirements in a policy, and implement controls that meet the requirements.

Ensure that the chosen threshold is defined in the organization's IA management policy and be prepared to demonstrate system settings that enforce the policy. In addition to using technology to disable unused accounts, review accounts periodically (organizationally defined) and verify that they were disabled by practice (for example, on an employee's last day) or automatically when the time limit was reached.

## IA.L2-3.5.7

CMMC Short Name: Password Complexity

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

NIST SP 800-171 Reference: 3.5.7

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1d | Password strength and reuse restrictions are defined and enforced |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1d will likely provide a capability similar to IA.L2-3.5.7. Ensure that password requirements are well defined and communicated in a User Policy with your IA policy. Configure systems to require the same complexity definition, and prohibit incremental passwords, defined words, and sequential or repeating characters.

In general, longer is better and passphrases, rather than passwords, are recommended. System and privileged accounts should require a much higher complexity than user accounts. Most in the industry agree that longer, more complex passwords, coupled with MFA, are preferable and more secure than requiring frequent password changes.

## IA.L2-3.5.8

CMMC Short Name: Password Reuse

Prohibit password reuse for a specified number of generations.

NIST SP 800-171 Reference: 3.5.8

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-1d | Password strength and reuse restrictions are defined and enforced |

### Discussion

Fully Implementing or Largely Implementing ACCESS-1d will likely provide a capability similar to IA.L2-3.5.8. Defining these requirements in documentation such as an IA policy will serve as a basis to enforce reuse restrictions for those implementing controls.

Document an organization's reuse policy and ensure that it Is communicated throughout an organization. Verify that systems are configured to enforce the requirement. Generational reuse is related to password change frequency and complexity. Collectively, the way to approach this needs to support the business and to encourage security.

## IA.L2-3.5.9

CMMC Short Name: Temporary Passwords

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

NIST SP 800-171 Reference: 3.5.9

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice, but it is the default on many IT systems. Organizations can use this feature to allow new users, or users who requested a password reset, to create a new password when they first log in to the network. An IT help desk can provide users with a temporary password that allows them access to the network, but forces them to reset the password immediately before accessing system resources.

Ensure that you have not changed a setting that removes the password change requirement on initial login. Make sure that policies reflect the need for password change at first login.

## IA.L2-3.5.10

CMMC Short Name: Cryptographically-Protected Passwords

Store and transmit only cryptographically-protected passwords.

NIST SP 800-171 Reference: 3.5.10

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5d will likely provide a capability similar to IA.L2-3.5.10. Organizations should consider the assets that are within the scope of a CMMC assessment and ensure that they meet this requirement.

Storing and transmitting cryptographically protected passwords are likely the default behavior of most assets. Although this may not be true for some OT assets, those assets would not be assessed against this CMMC requirement. It is important to note that organizations are required to have risk-based security policies, procedures, and practices for the assets.

## IA.L2-3.5.11

CMMC Short Name: Obscure Feedback

Obscure feedback of authentication information.

NIST SP 800-171 Reference: 3.5.11

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice, but this system behavior is the default behavior of most assets.

Most assets display a generic character when a user enters a password by default. Assets may not need additional configuration to meet this CMMC requirement, but an organization should consider documenting this requirement in related policies.

# Incident Response

## IR.L2-3.6.1

CMMC Short Name: 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 Reference: 3.6.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| RESPONSE-2a | Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner |
| RESPONSE-3d | Cybersecurity incident response plans that address all phases of the incident lifecycle are established and maintained |
| RESPONSE-3e | Cybersecurity incident response is executed according to defined plans and procedures |
| RESPONSE-5b | Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain |

### Discussion

Fully Implementing or Largely Implementing RESPONSE-2a, RESPONSE-3d, RESPONSE-3e and RESPONSE-5b will likely provide a capability similar to the one required by IR.L2-3.6.1. This CMMC requirement requires an organization to establish an incident handling program that covers all phases of an incident. Included in NIST Special Publication 800-61 Rev. 2 *Computer Security Incident Handling Guide* is detailed information on building an incident response capability, including considerations for building an incident response team, necessary activities for each phase of an incident, and information sharing best practices.

Establishing an incident handling capability begins with the development of a policy and a plan that guide the creation of the program and give authority to the program lead. These documents provide the direction necessary to hire or assign individuals to the team and the justification for the purchase of necessary tools and equipment. Next, the team should draft procedures that outline activities like incident reporting, incident declaration, and incident response. These procedures will ensure that responses to incidents are performed consistently and account for important considerations, such as chain of custody, reporting requirements, and incident data protection requirements. An organization should consider activities to be performed after an incident, such as lessons learned activities and updates to policies, plans, and procedures to prepare for and address future incidents more effectively.

## IR.L2-3.6.2

CMMC Short Name: Incident Reporting

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

NIST SP 800-171 Reference: 3.6.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| RESPONSE-1a | Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner |
| RESPONSE-2f | There is a repository where cybersecurity events and incidents are documented and tracked to closure |
| RESPONSE-2g | Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d) |
| RESPONSE-3c | Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner |
| RESPONSE-3f | Cybersecurity incident response plans include a communications plan for internal and external stakeholders |

### Discussion

Fully Implementing or Largely Implementing RESPONSE-1a, RESPONSE-2f, RESPONSE-2g, RESPONSE-3c, and RESPONSE-3f would likely provide a capabilities similar to those that are required by IR.L2-3.6.2. This practice requires organizations to develop a method of tracking and documenting incidents and document the parties that must be notified in the event of an incident.

To effectively manage incidents, an organization should establish a method for the incident lead to track and document information related to an incident. An organization can implement a tracking system with workflows to ensure that necessary steps in the incident response process are performed and to enable higher-level reporting to leadership. An incident response team can also use such a system in its incident notification to organization officials, and to know when an incident requires notification to external authorities.

## IR.L2-3.6.3

CMMC Short Name: Incident Response Testing

Test the organizational incident response capability.

NIST SP 800-171 Reference: 3.6.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| RESPONSE-3g | Cybersecurity incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events |
| RESPONSE-3k | Cybersecurity incident response personnel participate in joint cybersecurity exercises with other organizations |
| RESPONSE-4i | Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events |

### Discussion

Organizations that have Fully Implemented or Largely Implemented both RESPONSE-3g, RESPONSE-3k, and RESPOSNE-4i will likely have a capability similar to the requirements of IR.L2-3.6.3. Performing tests that validate the effectiveness organization's incident response capability will help identify potential gaps or deficiencies in plans and procedures.

An organization should consider documenting the frequency for completion of incident response testing, e.g., annually; criteria for testing; and required activities for addressing findings discovered during testing. For example, when conducting an incident response test, the team discovers that the tool used for producing forensic images does not support a newly acquired OT asset. This provides justification for research, acquisition, and testing of a new or additional tool that could perform this function.

# Maintenance

## MA.L2-3.7.1

CMMC Short Name: Perform Maintenance

Perform maintenance on organizational systems.

NIST SP 800-171 Reference: 3.7.1

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3i | Maintenance and capacity management activities are performed for all assets within the function |

### Discussion

If an organization has Fully Implemented or Largely Implemented ARCHITECTURE-3i, it can have a capability similar to MA.L2-3.7.1, but should its change management practices to ensure that they address the maintenance-specific requirements of CMMC.

Organizations should develop a maintenance schedule for their assets to meet both the guidelines set forth by manufacturers and the operational requirements. Examples of maintenance include activities such as patching vulnerabilities, vendor-recommended updates, and physical maintenance of assets. Change management practices can include the requirement to document the changes performed in a centralized repository. Changes performed by both an organization and third parties should documented. An organization should consider including changes to hardware, software, and firmware in change management practices.

## MA.L2-3.7.2

CMMC Short Name: System Maintenance Control

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

NIST SP 800-171 Reference: 3.7.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-4a | Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner |
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner |
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| THIRD-PARTIES-1b | Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to the delivery of the function are identified, at least in an ad hoc manner |
| THIRD-PARTIES-2e | More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties |

### Discussion

Fully Implementing or Largely Implementing ASSET-4a, ACCESS-2a, ACCESS-3a, THIRD-PARTIES-1b, and THIRD-PARTIES-2e can provide a capability similar to MA.L2-3.7.2, but an organization should review their review change management practices to ensure that they address the maintenance-specific requirements of CMMC.

Performing system maintenance helps ensure that systems continue to operate as expected and operational requirements can be sustained. Organizations should implement controls that mitigate potential risks introduced by system maintenance, such as applying a patch that degrades system performance, or running a tool that impacts network performance. Change management practices should define permitted tools, techniques, and mechanisms used to conduct system maintenance. An organization should consider which roles should be responsible for conducting system maintenance, then implement access controls to limit these actions to specific internal or third-party personnel.

## MA.L2-3.7.3

CMMC Short Name: Equipment Sanitization

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

NIST SP 800-171 Reference: 3.7.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ASSET-1h | Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life |

### Discussion

Fully Implementing or Largely Implementing ASSET-1h could provide a capability similar to MA.L2-3.7.3, but special consideration should be given to the CUI-specific requirements of this practice.

Maintenance of some equipment may need to be performed off-site. For example, a controller may need to be sent to a vendor for diagnosis. Sensitive information should be removed from assets that are not under the control of an organization. This practice is specifically focused on CUI, but an organization should consider this activity for other information that it considers sensitive. For CUI, refer to the guidance in NIST Special Publication 800-88 Rev. 1 *Guidelines for Media Sanitization*.

## MA.L2-3.7.4

CMMC Short Name: Media Inspection

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

NIST SP 800-171 Reference: 3.7.4

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3g | The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3g could provide a capability similar to MA.L2-3.7.4, but organizations should review their change management practices to ensure that they address the maintenance and CUI-specific requirements of CMMC.

Maintenance of assets may require execution of diagnostic or test applications from removeable media by an organization or a third party. Removeable media should be tested to verify that it does not contain malicious code prior to connecting to organizational assets, particularly to systems that process, store, or transmit CUI.

## MA.L2-3.7.5

CMMC Short Name: 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 Reference: 3.7.5

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-4e | Changes and updates are implemented in a secure manner |
| ACCESS-1f | Identities are deprovisioned within organization-defined time thresholds when no longer required |
| ACCESS-1h | Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access) |

### Discussion

Fully Implementing or Largely Implementing ASSET-4e, ACCESS-1f and ACCESS-1h could provide a capability similar to MA.L2-3.7.5, but organizations should review their access control practices to ensure that they address the maintenance-specific requirements of CMMC.

An organization or a third party can conduct some system maintenance remotely. For example, staff responsible for maintaining assets are located at a central facility and are responsible for maintaining equipment at other satellite facilities. An organization should ensure that additional protections are implemented for performing these sensitive actions remotely. This could be by a remote desktop session that requires multifactor authentication to initiate the connection and is terminated when maintenance is complete.

## MA.L2-3.7.6

CMMC Short Name: Maintenance Personnel

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

NIST SP 800-171 Reference: 3.7.6

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3j | Physical access is monitored to identify potential cybersecurity events |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3j could provide a capability similar to MA.L2-3.7.6, but organizations should review access control procedures to ensure that they meet the CMMC maintenance-specific requirements.

Sensitive areas of a facility, such as process control rooms, should have restricted physical access requirements to limit access to only those employees who need it to fulfill their job responsibilities. There may be an operational need to authorize employees with other duties, such as building maintenance, to access these areas. In both instances, these employees have prior physical access authorization.

In addition, organizations should consider procedures for supervising those who do not have authorization to, but must access, a restricted area to perform maintenance. For example, a vendor representative is onsite to perform maintenance of process control devices. While this maintenance is being performed, the representative must be escorted by someone who verifies the actions they are taking to ensure that they do not impact the overall process.

# Media Protection

## MP.L2-3.8.3

CMMC Short Name: Media Disposal

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

NIST SP 800-171 Reference: 3.8.3

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ASSET-1h | Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life |
| ASSET-2h | Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements |

### Discussion

Fully Implementing or Largely Implementing ASSET-1h and ASSET-2h could provide some capability of MP.L2-3.8.3, but organizations should review the CUI-specific requirements of this CMMC requirement. Media must be properly sanitized or destroyed prior to disposal or reuse. In addition to shredding paper media, devices that store CUI should be physically destroyed or logically wiped or overwritten depending on the type of device. In addition to common storage devices such as disk drives and DVDs, organizations should also consider USB drives, mobile phones and tablets, and printers, because these devices can store data, and need to be handled properly until control is surrendered.

NIST Special Publication 800-88 Rev. 1 *Guidelines for Media Sanitization* provides guidance on media sanitization. Many organizations incorrectly reference legacy instructions in DoD 5220.22 in their media disposal policies. Ensure that you structure your disposal requirements with respect to the NIST instructions.

## MP.L2-3.8.1

CMMC Short Name: Media Protection

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

NIST SP 800-171 Reference: 3.8.1

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| ACCESS-3d | Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access) |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3a and ACCESS-3d could provide a capability similar to MP.L2-3.8.1, but organizations should review the CUI-specific requirements of this practice. CMMC requires physical access control to CUI, in addition to logical limits to digitally stored CUI. This includes hardcopy CUI, physical devices that contain CUI, and digitally stored CUI as well. Controlling access to physical CUI includes the need to inventory it and monitoring who has had physical access to it.

Methods of tracking CUI access to physical media include storage in locked containers, electronic locks on doors (i.e., badging), and access logs. In addition to other types of controlled information, consider including CUI as a category of information protected in access and information assurance policies.

## MP.L2-3.8.2

CMMC Short Name: Media Access

Limit access to CUI on system media to authorized users.

NIST SP 800-171 Reference: 3.8.2

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| ACCESS-3b | Physical access privileges are revoked when no longer needed, at least in an ad hoc manner |
| ACCESS-3c | Physical access logs are maintained, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3a, ACCESS-3b, and ACCESS-3c will likely provide a capability similar to MP.L2-3.8.2, but organizations should review the CUI-specific requirements of this CMMC requirement.

This practice is an extension of MP.L2-3.8.1, In addition to protecting the media, the practice requires organizations to:

- have policies and procedures in place to determine who has access to the physical CUI,
- track who accesses the media (check-in/check-out) and who accesses controlled areas containing protected media.

## MP.L2-3.8.4

CMMC Short Name: Media Markings

Mark media with necessary CUI markings and distribution limitations.

NIST SP 800-171 Reference: 3.8.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice because of the CUI-specific nature of the requirements. CUI requires special markings, each specific to the CUI category. The U.S. National Archives and Records Administration (NARA) is the executive agent for CUI, and has a marking handbook available on the NARA CUI program page along with training material instructions how to correctly mark CUI.

Guidance should cover physical and electronic marking; include this material in your CUI handling procedures and user training. The DoD CUI website provides additional CUI information, including details about mandatory CUI training.

## MP.L2-3.8.5

CMMC Short Name: Media Accountability

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

NIST SP 800-171 Reference: 3.8.5

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice because of the CUI-specific nature of the requirements. In addition to controlling access to CUI, this practice includes the requirement for accountability during transport outside of controlled areas. In addition to maintaining a check-in/check-out system, organizations need a mechanism to assign responsibility and accountability for the media when it is no longer within the physical confines of their controlled area.

The NARA CUI program page provides guidance for tamper-evident packaging and labeling CUI for shipment when not under direct control of an authorized individual. MP.L2-3.8.6 provides additional guidance regarding encryption on devices containing CUI.

## MP.L2-3.8.6

CMMC Short Name: 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 Reference: 3.8.6

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |
| ARCHITECTURE-5g | The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5d and ARCHITECTURE-5g will likely provide capabilities similar to MP.L2-3.8.6, but organizations should review the CUI-specific requirements of this CMMC requirement. CMMC imposes an additional requirement: encryption modules must be FIPS 140-2 validated. The NIST CMVP website lists FIPS-validated modules. FIPS 140-3 is in the process of being phased in. Look for updates to CMMC assessment guides as NIST updates the SP 800 series documents.

NIST SP 800-111 *Guide to Storage Encryption Technologies for End User Devices* provides guidance on storage encryption technologies for end-user devices.

## MP.L2-3.8.7

CMMC Short Name: Removable Media

Control the use of removable media on system components.

NIST SP 800-171 Reference: 3.8.7

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3g | The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3g will likely provide the same capability as MP.L2-3.8.7. At a minimum, an organization should communicate its policy to all users, and document it in its acceptable-use policy, IT User Policy, and/or media control policy. Use of removeable media can increase the risk of data exfiltration, and introduces an additional threat vector. Organizations should consider implementing technical controls to restrict the use of these devices. In addition to operating system controls, numerous types of software can limit the ability to plug in storage devices without affecting the USB port use with other devices.

If business needs dictate the use of portable storage devices, use only devices that an organization issued. This can be enforced through the same configurations that restrict the device. When transporting CUI on portable storage devices, consider a solution designed specifically for that purpose. The market offers several solutions that enforce FIPS-validated encryption, restrict use to only the authorized devices, and monitor usage of the USB drives.

## MP.L2-3.8.8

CMMC Short Name: Shared Media

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

NIST SP 800-171 Reference: 3.8.8

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3g | The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3g may provide some capability of MP.L2-3.8.8, but organizations should review the requirements of this CMMC requirement to determine if additional administrative or technical controls are necessary to meet this practice.

If portable storage devices are prohibited as part of MP.L2-3.8.7, then this practice is covered. If portable storage devices are allowed then, at a minimum, an organization's policy should prohibit unknown devices but, preferably, have technology in place to prevent the use of unknown devices. See MP.L2-3.8.7.

## MP.L2-3.8.9

CMMC Short Name: Protect Backups

Protect the confidentiality of backup CUI at storage locations.

NIST SP 800-171 Reference: 3.8.9

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| RESPONSE-4j | Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data |
| RESPONSE-4k | Data backups are logically or physically separated from source data |
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implementing or Largely Implementing REPONSE-4j, and RESPONSE-4k, and ARCHITECTURE-5d will likely provide a capability similar to MP.L2-3.8.9, but organizations should consider the CUI-specific requirements of this CMMC requirement. Backup storage facilities should provide at least the same level of protection as the facility where the data is hosted. This can be using the same physical and logical controls employed at the host site. To be effective, a backup should be held at an alternate site, where the practice may present additional implementation challenges.

While in transit–whether carrying a physical device or transmitting the backup to a cloud facility–the backup containing CUI must be encrypted using a FIPS-validated module or afforded alternate physical protections. Alternate physical protections apply only to the transportation of a physical storage device. When evaluating cloud backup options, ensure that the backup is encrypted in transit using a FIPS-140-2-validated module. Most every backup option supports encryption, however, not all use validated modules.

# Personnel Security

## PS.L2-3.9.1

CMMC Short Name: Screen Individuals

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

NIST SP 800-171 Reference: 3.9.1

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| WORKFORCE-1a | Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner |
| WORKFORCE-1c | Personnel vetting is performed at hire and periodically for positions that have access to assets that are important to the delivery of the function |
| WORKFORCE-1f | Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk |

### Discussion

Fully Implementing or Largely Implementing WORKFORCE-1a, WORKFORCE-1c, and, WORKFORCE-1f will likely provide a capability similar to PS.L2-3.9.1, but the CUI-specific requirements of this practice should be considered. An organization may need to modify existing vetting procedures to ensure that they meet this requirement.

For example, an organization restricts CUI to specific workstations in a physically separated enclave in the facility. The door has a badge reader to physically control access, along with signage that announces access restrictions. Some employees in low-risk positions are not subject to background checks upon hire. When employees request access to the enclave, the security office ensures that they have undergone a background check and have completed a computer-based training module that details the policies that apply to the CUI enclave.

## PS.L2-3.9.2

CMMC Short Name: Personnel Actions

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

NIST SP 800-171 Reference: 3.9.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2b | Logical access privileges are revoked when no longer needed, at least in an ad hoc manner |
| WORKFORCE-1b | Personnel separation procedures address cybersecurity, at least in an ad hoc manner |
| WORKFORCE-1d | Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate |

### Discussion

Fully Implementing or Largely Implementing WORKFORCE-3b, WORKFORCE-3d, and ACCESS-2b will likely provide a capability similar to PS.L2-3.9.2, but the CUI-specific requirements of this CMMC requirement should be considered. To meet the assessment objectives of this CMMC requirement, controls must be implemented that terminate access to CUI for employees who change job roles or leave an organization.

For example, an organization is preparing to gain work that requires CMMC certification. The security team is working with the enterprise IT team on policies and procedures for employee transfer and termination. The teams develop a process for each situation that is triggered by a notification from the HR team that an employee action has occurred. After the notification, access is revoked to an organization's network, systems, and applications if an employee is being terminated. The process includes steps to ensure that all equipment and physical access devices (e.g., keys, badges) are returned, and an exit interview is conducted.

# Physical Protection

## PE.L2-3.10.1

CMMC Short Name: Limit Physical Access

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

NIST SP 800-171 Reference: 3.10.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| ACCESS-3d | Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access) |
| ARCHITECTURE-3a | Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3a, ACCESS-3d, and ARCHITECTURE-3a will likely provide the same capabilities as PE.L2-3.10.1. Limiting physical access to organizational assets is important to ensure that an organization can meet security and safety requirements.

Organizations should implement physical access controls that reduce the risk of an incident resulting from unauthorized access. The risk may vary based upon the assets within a physical space. Organizations should take a risk-based approach in determining the level of physical access controls necessary to reduce risk to acceptable levels. For example, a control room that monitors and controls assets throughout a region presents a greater risk than a storage facility. Organizations should consider which individuals should have access to systems, equipment, and operating environments, and provide access only to individuals who need it based on their job responsibilities.

## PE.L2-3.10.3

CMMC Short Name: Escort Visitors

Escort visitors and monitor visitor activity.

NIST SP 800-171 Reference: 3.10.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3h | Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3h will likely provide the same capability as PE.L2-3.10.3.

Organizations should implement controls to restrict and monitor unauthorized individuals from physical access to facilities. There may be exceptions when portions of a facility may be open to the public, for example, a desk where a customer can pay a bill. An organization should have policies and procedures in place for situations when a visitor needs to access restricted areas of a facility, for example, for a safety inspection. Visitors should always be escorted in restricted areas for safety and security. An organization should implement a process for visitor sign-in and sign-out of a facility, and be visitor badge assignment.

## PE.L2-3.10.4

CMMC Short Name: Physical Access Logs

Maintain audit logs of physical access.

NIST SP 800-171 Reference: 3.10.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3c | Physical access logs are maintained, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3c will likely provide the same capability as PE.L2-3.10.4.

An organization should implement a method to log physical access of authorized individuals and visitors. There are a variety of ways to implement this, including a paper sign-in log or an automated log generated by a physical access system. The logs must be protected and retained to meet organizational retention requirements.

## PE.L2-3.10.5

CMMC Short Name: Manage Physical Access

Control and manage physical access devices.

NIST SP 800-171 Reference: 3.10.5

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| ACCESS-3b | Physical access privileges are revoked when no longer needed, at least in an ad hoc manner |
| ACCESS-3d | Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access) |
| ACCESS-3i | Physical access privileges are reviewed and updated |
| ARCHITECTURE-3a | Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3a, ACCESS-3b, ACCESS-3d, ACCESS-3i, and ARCHITECTURE-3a will likely provide the same capability as PE.L2-3.10.5. Similar to assigning logical access identities, an organization should assign physical access devices to authorized employees to control physical access.

It is important that an organization has a record of who has been assigned such assets as keys, badges, and combinations to locks. An organization can meet this requirement by keeping a log that employees sign when they receive one of the assets. Employees should be held accountable for protecting the assets, and instructed to use them only for authorized purposes. An organization should implement procedures for revoking these assets when an employee transfers or is terminated. In addition, an organization may need to consider processes for changing locks or combinations in situations when an authorized individual does not control an asset.

## PE.L2-3.10.2

CMMC Short Name: Monitor Facility

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

NIST SP 800-171 Reference: 3.10.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-3a | Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner |
| ACCESS-3j | Physical access is monitored to identify potential cybersecurity events |
| ARCHITECTURE-3j | The physical operating environment is controlled to protect the operation of assets within the function |

### Discussion

Fully Implementing or Largely Implementing ACCESS-3a, ACCESS-3i, and ARCHITECTURE-3j will likely provide some of the capabilities necessary to meet PE.L2-3.10.2, but an organization should review the support infrastructure requirements of this CMMC requirement to determine if additional protections and monitoring need to be implemented to meet the requirements of this CMMC requirement.

This CMMC requirement requires implementation of controls to protect and monitor the physical facility, as well as the support infrastructure. There can be a variety of access controls, such as fences, doors with locks or badge readers, and guard checkpoints. It is equally important to monitor physical access, which can be accomplished through such methods as video cameras and access logs. An organization should review the controls for protecting and monitoring the physical space to determine if they provide the same protections for support infrastructure, such as communication cables and power lines.

## PE.L2-3.10.6

CMMC Short Name: Alternative Work Sites

Enforce safeguarding measures for CUI at alternate work sites.

NIST SP 800-171 Reference: 3.10.6

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ASSET-2e | The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements) |
| ACCESS-3d | Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access) |
| ARCHITECTURE-1f | The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets |
| ARCHITECTURE-5b | All data at rest is protected for selected data categories |

### Discussion

Fully Implementing or Largely Implementing ASSET-2e, ACCESS-3d, ARCHITECTURE-1f, and ARCHITECTURE-5b may provide a capability similar to PE.L2-3.10.6, but organizations should review the CUI-specific requirements of this CMMC requirement.

Organizations should ensure that policies and procedures are implemented for safeguarding sensitive information (e.g., CUI) at alternate work sites, such as at an employee's home or at a hotel if an employee is traveling. An organization should implement a policy that requires employees to inspect an alternate work site to ensure that it meets requirements similar to their normal workspace. For example, an organization may require that laptop displays are turned away from open windows. In addition, to reduce the risk of unauthorized disclosure, assets that may be used to access CUI should have controls such as full disk encryption, endpoint protections, and multifactor authentication for VPN access.

# Risk Assessment

## RA.L2-3.11.1

CMMC Short Name: 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 trans

NIST SP 800-171 Reference: 3.11.1

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| RISK-2b | A defined method is used to identify cyber risks |
| RISK-2g | Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events |
| RISK-2h | Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction |
| THIRD-PARTIES-1c | A defined method is followed to identify risks arising from suppliers and other third parties |

### Discussion

Fully Implementing or Largely Implementing RISK-2b, RISK-2g, RISK-2h, and THIRD-PARTIES-1c will likely provide a capability similar to RA.L2-3.11.1, but organizations should review the CUI-specific requirements of this CMMC requirement.

The CMMC requirement specifically calls out risks related to CUI, but it indicates that it should be only one category of risk in an organization's overall Risk Assessment. And, while C2M2 specifically mentions cyber risks, CMMC casts a wider net and includes such items as business processes and natural disasters.

Organizations should consider how Risk Assessment activities relate to other governing policies, such as the Disaster Recovery Plan or Business Continuity Plan. The RA should be reviewed and updated, as needed, and at least once annually, it should also be reviewed following any significant change to an organization's risk profile or appetite for risk.

NIST SP 800-30 *Guide for Conducting Risk Assessments* provides guidance on conducting risk assessments.

## RA.L2-3.11.2

CMMC Short Name: 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 Reference: 3.11.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| THREAT-1f | Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events |

### Discussion

Fully Implementing or Largely Implementing THREAT-1f will likely provide the same capability as RA.L2-3.11.2. In both C2M2 and CMMC, organizations are expected to perform vulnerability scanning when there are significant system changes, new vulnerabilities are disclosed, and on an organizationally defined frequency. In their asset maintenance or risk management policies, organizations should consider documenting the scan interval and be prepared to show evidence (i.e., the scan reports) that they performed them.

In general, monthly scanning is regarded as a reasonable interval and is effective. When significant zero-day threats are announced, organizations should consider running out of cycle scans. Because CMMC requires scanning systems and applications, organizations should consider an approach that covers all devices within the scope of a CMMC assessment. The best approaches use a combination of agent-based scans, when an agent resides on the endpoint and provides “continuous” scanning, and enterprise scans, when a scanner runs across the environment to check devices that do not host an agent.

When using cloud services, typically the CSP blocks independent scans of their environment, but the services should be performing them as part of their SLAs and/or contracts. With the continued use of hybrid and remote work environments, traditional scanning does not always capture devices not connected to the organizational infrastructure. Ensure that your approach does not exclude these remote devices. Although not specifically designed as vulnerability scanners, many EDR/XDR and SIEM tools include that capability as a byproduct of their core service and can greatly contribute to a better cyber posture.

## RA.L2-3.11.3

CMMC Short Name: Vulnerability Remediation

Remediate vulnerabilities in accordance with risk assessments.

NIST SP 800-171 Reference: 3.11.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| THREAT-1c | Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner |
| THREAT-1d | Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner |
| THREAT-1g | Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly |
| THREAT-1m | Mechanisms are established and maintained to receive and respond to reports from the public or external parties of potential vulnerabilities related to the organization's IT and OT assets, such as public-facing websites or mobile applications |

### Discussion

Fully Implementing or Largely Implementing THREAT-1c, THREAT-1d, THREAT-1g, and THREAT-1m will likely provide the same capability as RA.L2-3.11.3. A major distinction between C2M2 and CMMC is the level of structure and formality expected in CMMC; ad-hoc remediation is not acceptable in an assessment. An organization's remediation plan should be tightly woven in with the overall Configuration Management Plan, Risk Assessment, and maintenance strategy.

Because not all vulnerabilities have equal impact, an organization's ability to patch or mitigate them is largely dependent on their severity; the potential impact to an organization if exploited; and the business impact to deploy the fix. Guidelines to help in the decision process should be part of the Risk Assessment.

An organization should track in its risk register and POA&M all vulnerabilities that it doesn't fix, including those that it implemented a mitigation for, but has to make an additional fix to eliminate the vulnerability.

# Security Assessment

## CA.L2-3.12.1

CMMC Short Name: 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 Reference: 3.12.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| RISK-4c | Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks |

### Discussion

Fully Implementing or Largely Implementing RISK-4c will likely provide some of the capability of CA.L2-3.12.1, but the additional assessment frequency requirement of the CMMC requirement should be considered.

Organizations should evaluate whether security controls implemented to protect their assets are still effective in addressing the changing threat landscape, organizational requirements, and regulatory requirements. Documenting a frequency by which these evaluations should be performed and executing these evaluations according to that schedule will give greater assurance that security controls and countermeasures are sufficient to reduce potential risks to organizational risk tolerances. Organizations should also consider documenting a standard to be used to plan, execute, and communicate the results these evaluations to produce consistent and expected results.

## CA.L2-3.12.2

CMMC Short Name: 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 Reference: 3.12.2

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| RISK-2i | Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities) |
| RISK-2l | Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks |
| RISK-4a | Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner |
| RISK-4b | A defined method is used to select and implement risk responses based on analysis and prioritization |

### Discussion

Fully Implementing or Largely Implementing RISK-2i, RISK-2l, RISK-4a, and RISK-4b will likely provide a capability similar to CA.L2-3.13.2.

After identifying and analyzing risks, organizations should choose an appropriate risk response, which may include deferring the implementation of a control to directly address a risk. The choice may be based on constraints, such as funding, resource availability, or scheduling. To meet the requirements of this CMMC requirement, organizations should develop documentation to address planned remediations that meets the typical requirements for a plan of action document. The CMMC Level 2 Assessment Guide details the following potential requirements:

- ownership of who is accountable for ensuring the plan's performance;
- specific steps or milestones that are clear and actionable;
- assigned responsibility for each step or milestone;
- milestones to measure plan progress; and
- completion dates.

NIST provides a POA&M template on the NIST SP 800-171 Rev. 2 publication page.

## CA.L2-3.12.3

CMMC Short Name: Security Control Monitoring

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

NIST SP 800-171 Reference: 3.12.3

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| RISK-4c | Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks |
| RISK-4d | Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated, and risk tolerances are not exceeded |

### Discussion

Fully Implementing or Largely Implementing RISK-4c and RISK-4d will likely provide the same capability as CA.L2-3.12.3.

CA.L2-3.12.3 extends the periodic review of control effectiveness in CA.L2-3.12.1 to perform the evaluations on an ongoing basis. An organization should consider developing a defined process for evaluating and analyzing control effectiveness at a frequency that supports organizational risk management decisions. In addition, an organization should consider methods for communicating the results that meet stakeholder requirements to enable efficient decision making.

## CA.L2-3.12.4

CMMC Short Name: 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 Reference: 3.12.4

DoD 800-171 Assessment Methodology Point Value:

The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-1b | A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture |
| ARCHITECTURE-1c | A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization |
| ARCHITECTURE-1f | The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-1b, ARCHITECTURE-1c, and ARCHITECTURE-1f will likely provide a capability similar to CA.L2-3.12.4, but organizations should consider the CMMC-specific requirements of this practice.

SSPs are one of the primary documents that organizations are required to develop and maintain when operating a covered contractor information system, and are required as part of a CMMC assessment. Organizations may consider overlapping requirements between a typical SSP and current cybersecurity architecture documentation. NIST provides an SSP template on the NIST SP 800-171 Rev. 2 publication page.

# Systems and Communications Protection

## SC.L2-3.13.1

CMMC Short Name: 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.

NIST SP 800-171 Reference: 3.13.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2d | Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements |
| ARCHITECTURE-2f | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) |
| ARCHITECTURE-2g | Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2b, ARCHITECTURE-2f, and ARCHITECTURE-2g will likely provide a capability similar to SC.L2-3.13.1. An organization should consider the location of network protection devices to ensure that they are implementing adequate monitoring and control of network traffic at internal and external network boundaries.

Network protection devices such as firewalls are vital to controlling network traffic and protecting the network from unwanted or malicious traffic. Other devices such as gateways and routers manage the flow of traffic and can be used to implement subnets. It is important for organizations to first evaluate, then document system boundaries to determine if current network protection devices provide adequate security for sensitive information. Organizations may need to implement additional controls to meet operational and protection requirements, such as:

- firewalls to restrict traffic at internal or external boundaries;
- a web proxy to shield users from direct interaction with websites; and
- encrypted tunnels for secure data transmission.

## SC.L2-3.13.5

CMMC Short Name: Public-Access System Separation

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

NIST SP 800-171 Reference: 3.13.5

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2d | Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2d may provide a capability similar to SC.L2-3.13.5, but an organization should give additional consideration to assets that are accessible publicly. It is important to separate these assets from the internal network because they could serve as an initial intrusion point.

Organizations should identify assets that are publicly accessible, and consider documenting this information in artifacts such as an asset inventory or documentation for the network architecture. After identifying the assets, an organization should determine whether sufficient segmentation is in place to separate the assets from the internal network. It is common practice to place all publicly accessible assets in a separate demilitarized zone (DMZ) segment of the network that is outside the internal network. This architectural tactic helps mitigate the risk that an attacker who compromises a publicly accessible system moves laterally. An organization may consider testing, for example, an external penetration test, to identify additional assets that are accessible from the internet.

## SC.L2-3.13.2

CMMC Short Name: Security Engineering

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

NIST SP 800-171 Reference: 3.13.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-1c | A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization |
| ARCHITECTURE-1f | The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets |
| ARCHITECTURE-1g | Cybersecurity controls are selected and implemented to meet cybersecurity requirements |
| ARCHITECTURE-1i | Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events |
| ARCHITECTURE-4a | Software developed in-house for deployment on higher priority assets is developed using secure software development practices |
| ARCHITECTURE-4c | Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house |
| ARCHITECTURE-4d | All software developed in-house is developed using secure software development practices |
| ARCHITECTURE-4f | The architecture review process evaluates the security of new and revised applications prior to deployment |
| ARCHITECTURE-4h | Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to defined triggers, such as system changes and external events |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-1c, ARCHITECTURE-1f, ARCHITECTURE-1g, ARCHITECTURE-1i, ARCHITECTURE-4a, ARCHITECTURE-4c, ARCHITECTURE-4d, ARCHITECTURE-4f, and ARCHITECTURE-4h may provide some capabilities similar to SC.L2-3.12.2, but organizations should consider the necessary system-engineering-specific requirements of this CMMC requirement. Implementation of these C2M2 practices enables organizations to employ consistently system and network protections that meet protection requirements and produce secure software. Review the secure system engineer principles described in NIST SP 800-160 Vol. 1 *Systems Security*

*Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* for applicability to system development activities.

An organization's cybersecurity program should consider how cybersecurity requirements apply to different types of assets, and include documentation of these requirements in a cybersecurity architecture. The establishment of a cybersecurity architecture provides a reference for those implementing security controls to ensure that the controls meet defined cybersecurity requirements for an organization's assets. Similarly, an organization should establish requirements for developing secure software and use them to implement a process that enables developers to produce software that meets cybersecurity requirements. This process may include requirements such as

- separation between development and production environments;
- methods to identify potential risks to software;
- code review requirements;
- testing methods;
- and configuration requirements.

## SC.L2-3.13.3

CMMC Short Name: Role Separation

Separate user functionality from system management functionality.

NIST SP 800-171 Reference: 3.13.3

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2c | Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters) |
| ACCESS-2e | Logical access requirements incorporate the principle of separation of duties |
| ARCHITECTURE-2d | Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements |
| ARCHITECTURE-2h | All assets are segmented into distinct security zones based on cybersecurity requirements |
| ARCHITECTURE-3c | The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced |

### Discussion

Fully Implementing or Largely Implementing ACCESS-2c, ACCESS-2e, ARCHITECTURE-2d, ARCHITECTURE-2h, and ARCHITECTURE-3c will likely provide the same capability as SC.L2-3.13.3. The core of this CMMC requirement is the principle of least privilege, and requires additional logical or physical separation to enforce this principle.

Organizations should identify the system management activities necessary for operations, then determine the methods used to access these sensitive functions. It might be necessary to document in organizational policy which activities should only be completed from specific systems or with different credentials. This CMMC requirement requires additional separation of the management of systems through logical or physical means, to ensure that only a limited number of users have access to the sensitive functions. For example, a network security engineer needs to perform maintenance on a firewall and implement new rules based on threat intelligence. This may be completed by logging into a separate administrative account on a virtual machine connected to a specific VLAN that has access to the management interface of the firewall.

## SC.L2-3.13.4

CMMC Short Name: Shared Resource Control

Prevent unauthorized and unintended information transfer via shared system resources.

NIST SP 800-171 Reference: 3.13.4

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3e | Secure configurations are established and maintained as part of the asset deployment process where feasible |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3e may provide similar functionality to SC.L2-3.13.4. An organization should continually review the configuration of assets to ensure that mitigations are in place for newly discovered vulnerabilities.

This CMMC requirement could leverage other activities, for example, access controls, configuration baselines, and configuration hardening. Organizations should ensure that those activities are performed in a cohesive manner, perhaps through policy, to meet the requirements of this practice. Access controls may be used to prevent users from accessing the information of another user. Configuration baselines should be implemented to ensure that systems have the same controls in place to prevent unauthorized or unintended information transfer. System configurations and configuration baselines should be continuously reviewed and updated to mitigate newly discovered vulnerabilities that can allow the disclosure of unauthorized or unintended information.

## SC.L2-3.13.6

CMMC Short Name: 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 Reference: 3.13.6

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2f | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2f may provide the same capability as SC.L2-3.13.6, but configurations should be reviewed to ensure that they meet the specific requirements of this CMMC requirement.

Firewalls are a common way to restrict network traffic, but they are only as effective as the rules they use to filter traffic. This CMMC requirement requires firewalls and other network protection devices to be configured to deny all network traffic, and allow traffic only by exception. When implementing firewall rules, an organization must consider carefully the risk introduced by allowing different types of network traffic to traverse a boundary.

## SC.L2-3.13.7

CMMC Short Name: 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 Reference: 3.13.7

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3f | Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3f may provide the same capability as SC.L2-3.13.7, but an organization should review configurations to ensure that they meet the specific requirements of this CMMC requirement.

Split tunneling allows a system to establish a connection between two networks, such as a system simultaneously connecting to an organization's trusted VPN and n external network like the Internet. Implementation of controls to prevent split tunneling helps reduce the potential of an attacker exfiltrating information or using a trusted system as an initial point of entry into an organization's network. Preventing users from using split tunneling should be considered when creating both configuration baselines and an organization's cybersecurity architecture.

## SC.L2-3.13.8

CMMC Short Name: 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 Reference: 3.13.8

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5c | All data in transit is protected for selected data categories |
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5c and ARCHITECTURE-5d may provide some of the same capability as SC.L2-3.13.8, but an organization should review the CUI-specific requirements of this CMMC requirement.

Organizations must ensure that adequate controls are implemented to protect sensitive data such as CUI. Data in transit can be protected by such cryptographic mechanisms as a TLS connection between two systems. If cryptography is selected as the method to meet this CMMC requirement requirement, encryption must be implemented using FIPS-validated cryptography. The cryptographic module used to implement the algorithm must be validated under FIPS 140. Organizations can choose to implement physical protections instead of cryptographic ones in situations where encryption is not feasible or practical. Organizations can refer to the US government requirements for protected distribution systems (PDS) that protect unencrypted national security information. A PDS can have hardened or alarmed cable carriers, in addition to other requirements, based on the sensitivity of transmitted data and the threat environment.

## SC.L2-3.13.9

CMMC Short Name: 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 Reference: 3.13.9

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ASSET-3c | Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1f) |
| ARCHITECTURE-2c | Network protections are defined and enforced for selected asset types according to asset risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices) |
| ARCHITECTURE-3a | Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing ASSET-3c, ARCHITECTURE-2c, and ARCHITECTURE-3a may provide a capability similar to SC.L2-3.13.9, but an organization should review configurations to ensure that they meet the specific requirements of this CMMC requirement.

An unattended workstation can be leveraged by a malicious insider to exfiltrate information or perform actions on behalf of another user. Similarly, if a host is compromised, a remote attacker could take advantage of an active session to interact with another asset, such as another system or application. Organizations should consider timeout values for communications sessions, then define them in a document such as a policy. Configuration baselines should adhere to this requirement, and assets such as applications should be configured to terminate a connection after a period of inactivity.

## SC.L2-3.13.10

CMMC Short Name: Key Management

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

NIST SP 800-171 Reference: 3.13.10

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5e | Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5e will likely provide the same capability as SC.L2-3.13.10.

Cryptographic keys can be used to send a secure email, authenticate a remote access session, or encrypt information at rest. Much like a physical lock, these cryptographic keys are effective only if they are managed properly. An organization should have clearly defined policies and procedures for establishing and managing cryptographic keys. These may include

- the documentation of processes, such as the method a trusted individual uses to generate a key from an internal certificate authority;
- instructions for users to properly use a private key to encrypt an email; and
- the procedure to revoke a key.

## SC.L2-3.13.11

CMMC Short Name: CUI Encryption

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

NIST SP 800-171 Reference: 3.13.11

DoD 800-171 Assessment Methodology Point Value: 3 – if cryptography is not FIPS validated

5 – if no cryptography is employed

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5d may provide some of the same capability as SC.L2-3.13.11, but an organization should review the CUI-specific requirements of this CMMC requirement.

It is important to note that cryptography used to protect the confidentiality of CUI must be validated by the NIST Cryptographic Module Validation Program (CMVP). Organizations can consult the CMVP website for details about the CMVP and a listing of validated modules.

The focus of this practice is the use of validated cryptography. SC.L2-3.13.8 requires encryption for CUI in transit, and SC.L2-3.13.16 requires encryption for CUI is at rest. The CMMC Level 2 Assessment Guide states

> ...FIPS-validated cryptography is required to meet CMMC requirements that protect CUI when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access). Encryption used for other purposes, such as within applications or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated.

## SC.L2-3.13.12

CMMC Short Name: 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 Reference: 3.13.12

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice.

To conduct meetings with remote participants, organizations can implement collaborative computing devices, such as video conferencing systems, in conference rooms or other shared spaces. If sensitive information is discussed in a conference room, an attacker can potentially activate these devices to exfiltrate sensitive information. It is important to identify the devices, then ensure that they are configured to prohibit remote activation to mitigate against this attack. Similarly, devices should be used only if they present an indicator that they are in use, such as a light on a teleconference device, a screen that shows a meeting is in progress, or microphones with status lights. If a device does not have such indicators, an organization should consider compensating controls such as physical access restrictions or signage.

## SC.L2-3.13.13

CMMC Short Name: Mobile Code

Control and monitor the use of mobile code.

NIST SP 800-171 Reference: 3.13.13

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-3e | Secure configurations are established and maintained as part of the asset deployment process where feasible |
| ARCHITECTURE-3m | Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-3e and ARCHITECTURE-3m will likely provide a capability similar to SC.L2-3.13.13. In addition to technical controls, an organization needs to consider policies that document usage restrictions.

NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, defines mobile code as "[s]oftware programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient." Examples of mobile code include JavaScript, ActiveX, and VBScript. Because an attacker can use mobile code to execute malicious code, organizations should consider the types of mobile code that are necessary to meet business requirements.

An organization should document approved uses of mobile code, such as accounting functions that require a specific macro-enable spreadsheet or a Java application that is on an isolated system. Organizations should implement controls that enable the it to control and monitor the use of both approved and prohibited mobile code. This may be achieved through controls at different points, such as host configuration settings, host-based or network-based monitoring, or review of logs.

## SC.L2-3.13.14

CMMC Short Name: Voice over Internet Protocol

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

NIST SP 800-171 Reference: 3.13.14

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2f | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2f may provide a capability similar to SC.L2-3.13.14, but organizations should review the specific requirements of this CMMC requirement.

Voice over Internet Protocol (VoIP) technology can be implemented in place of traditional telephone service if an organization finds that VoIP presents implementation, feature, and cost benefits. Organizations should consider how current network protections can be leveraged to ensure that VoIP traffic is controlled and monitored like other network traffic. An organization should consider technical controls to prevent this disruption or interception of VoIP traffic, and to enforce the use of approved VoIP technologies. Organizations should also consider documenting the VoIP technologies approved for use, along with acceptable application of the technologies.

## SC.L2-3.13.15

CMMC Short Name: Communications Authenticity

Protect the authenticity of communications sessions.

NIST SP 800-171 Reference: 3.13.15

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2f | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2f will likely provide a capability similar to SC.L2-3.13.15. Organizations should ensure that systems and networking infrastructure are configured to meet this practice.

Ensuring the authenticity of communication sessions helps mitigate attacks that could intercept information from a legitimate communication session or spoof an intended recipient. For example, if wireless access is not encrypted, an attacker can intercept and potentially modify this traffic while in transit. Devices should be configured to use protocols that are able to authenticate a communication session, such as HTTPS or SSH.

## SC.L2-3.13.16

CMMC Short Name: Data at Rest

Protect the confidentiality of CUI at rest.

NIST SP 800-171 Reference: 3.13.16

DoD 800-171 Assessment Methodology Point Value: 1

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-5b | All data at rest is protected for selected data categories |
| ARCHITECTURE-5d | Cryptographic controls are implemented for data at rest and data in transit for selected data categories |
| ARCHITECTURE-5g | The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-5b, ARCHITECTURE-5d, and ARCHITECTURE-5g will like provide a capability similar to SC.L2-3.13.16, but an organization should review the CUI-specific requirements of this CMMC requirement.

Sensitive data, such as CUI, must be protected while at rest to mitigate against unauthorized disclosure. The selection of controls for protecting data at rest should be selected based on an organization's threat profile, and may include cryptography, logical access controls, and physical access controls. If cryptography is selected, the cryptographic module must be validated under FIPS 140. An organization may choose to implement physical and logical access restrictions in place of cryptography when encryption is not feasible or practical. For example, a database that contains CUI can be accessed only by workstations located in a physically controlled room.

# System and Information Integrity

## SI.L2-3.14.1

CMMC Short Name: Flaw Remediation

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

NIST SP 800-171 Reference: 3.14.1

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| THREAT-1a | Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner |
| THREAT-1b | Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner |
| THREAT-1c | Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner |
| THREAT-1d | Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner |

### Discussion

Fully Implementing or Largely Implementing THREAT-1a, THREAT-1b, THREAT-1c, and THREAT-1d may provide capabilities similar to SI.L2-3.14.1, but organizations should consider the specific time frame requirements of this CMMC requirement. Although C2M2 allows for an ad-hoc process for remediation, CMMC requires more structure. Organizations need to show that they have established time standards to identify, report, and correct flaws. Additionally, they have to demonstrate proof that their procedures permit meeting those timelines. If unable to meet them–if operational constraints prohibit restating a system–organizations should document the risk in a POA&M, then set a target for fixing it.

Flaws can be detected through a combination of vendor alerts, network and system scans, penetration tests, alerts, and events reported through system tools. Regardless of the source, organizations must ensure that the same processes are applied consistently to remediate the problem.

Although there is no precise definition of "timely manner," CISA has established a 14-day requirement for federal agencies to remediate vulnerabilities it adds to the Known Exploited Vulnerabilities Catalog. When prioritizing fixes, the CVE severity score is a good indicator of the impact and ease of exploiting a vulnerability.

## SI.L2-3.14.2

CMMC Short Name: Malicious Code Protection

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

NIST SP 800-171 Reference: 3.14.2

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ARCHITECTURE-2f | Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems (IDPS)) |
| ARCHITECTURE-2g | Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking) |
| ARCHITECTURE-3f | Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls) |
| ARCHITECTURE-3m | Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code |

### Discussion

Fully Implementing or Largely Implementing ARCHITECTURE-2f, ARCHITECTURE-2g, ARCHITECTURE-3f, and ARCHITECTURE-3m will likely provide the same capability to SI.L2-3.14.2. In the context of CMMC, this practice ties into configuration management policies because organizations need to identify locations that require protection. In addition to endpoint protection, prioritizing cloud services can be considered as filtering network traffic before it enters the network boundary, and could help achieve cybersecurity objectives.

Like C2M2, monitoring traffic and scanning as appropriate are also key to preventing malicious code from impacting assets. Organizations should ensure that mechanisms are in place to prevent malicious code from executing or spreading in the event that it manages to evade detection. Organizations should document the processes in place to demonstrate the layered defenses. If building or using custom applications for internal use, ensure that appropriate measures are in-place to mitigate the risk of malicious code being introduced.

## SI.L2-3.14.4

CMMC Short Name: Update Malicious Code Protection

Update malicious code protection mechanisms when new releases are available.

NIST SP 800-171 Reference: 3.14.4

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice, but it is likely that malicious code protection mechanisms meet this requirement by default. Ensure that deployed anti-malware solutions are updated regularly. Organizations hould define the update frequency and the tools configured to ensure that it is being updated. Some devices such as firewalls may require a manual update or restart, and occur on a less frequent basis than the anti-virus on a workstation.

## SI.L2-3.14.5

CMMC Short Name: 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.

NIST SP 800-171 Reference: 3.14.5

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| N/A | No related practices |

### Discussion

This CMMC requirement does not have a related C2M2 practice, but it is likely that malicious code protection mechanisms meet this requirement by default. In general, deployed anti-malware tools scan on access or in transit by default. Real-time scans can occur at multiple times: while browsing, in the cloud before it enters an organization's email system, and anytime a file is accessed.

CMMC requires that periodic full scans of systems are executed. Although there is no defined time for these scans, STIGs for some of the more common AV software require full scans at least weekly; some systems require a validation check before using the device to connect. Regardless of the method employed, organizations should ensure that it is documented and the tool is configured to perform the scan on that schedule.

## SI.L2-3.14.3

CMMC Short Name: Security Alerts & Advisories

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

NIST SP 800-171 Reference: 3.14.3

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| THREAT-1b | Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner |
| THREAT-1g | Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly |
| THREAT-2b | Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner |
| THREAT-2g | Identified threats are analyzed and prioritized and are addressed accordingly |
| THREAT-3a | Documented procedures are established, followed, and maintained for activities in the THREAT domain |

### Discussion

Fully Implementing or Largely Implementing THREAT-1b, THREAT-1g, THREAT-2b, THREAT-2g, and THREAT-3a will likely provide the same capability to SI.L2-3.14.4. A key part of CMMC is monitoring external sources of alerts and not relying on only items triggered in detection tools. US-CERT, vendor advisories, and subscription services are some of the sources to monitor.

Organizations should ensure that they have a documented process to notify affected stakeholders after a threat or vulnerability is identified so that appropriate corrective actions can be taken. External service providers should have similar processes in place.

## SI.L2-3.14.6

CMMC Short Name: 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 Reference: 3.14.6

DoD 800-171 Assessment Methodology Point Value: 5

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2i | Anomalous logical access attempts are monitored as indicators of cybersecurity events |
| SITUATION-2c | Monitoring and analysis requirements are established and maintained for the function and address timely review of event data |
| SITUATION-2d | Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments |
| SITUATION-2e | Alarms and alerts are configured and maintained to support the identification of cybersecurity events |

### Discussion

Fully Implementing or Largely Implementing ACCESS-2i, SITUATION-2c, SITUATION-2d, and SITUATION-2e will likely provide the same capability as SI.L2-3.14.6. Organizations should ensure that audit and retention practices are aligned with the requirements of this CMMC requirement.

## SI.L2-3.14.7

CMMC Short Name: Identify Unauthorized Use

Identify unauthorized use of organizational systems.

NIST SP 800-171 Reference: 3.14.7

DoD 800-171 Assessment Methodology Point Value: 3

### Related C2M2 Practices

| | |
|---|---|
| ACCESS-2i | Anomalous logical access attempts are monitored as indicators of cybersecurity events |
| SITUATION-2a | Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner |
| SITUATION-2b | Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner |
| SITUATION-2d | Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments |
| SITUATION-3f | A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function |

### Discussion

Fully Implementing or Largely Implementing ACCESS-2i, SITUATION-2a, SITUATION-2b, SITUATION-2d, and SITUATION-3f will likely provide a capability similar to SI.L2-3.14.7. Organizations should consider identifying and communicating acceptable and authorized system use requirements. This practice is closely related to SI.L2-3.14.6, which requires the use of tools to flag events on assets and the network.

Automation may be an ideal method to implement this practice. A SIEM tool, along with a strong process for responding to alerts, greatly improves overall cyber resiliency and makes for a strong implementation.

# APPENDIX B: APPLYING CMMC TO C2M2

This section is intended for organizations that have completed a CMMC assessment and want to complete a C2M2 self-evaluation. Organizations may consider C2M2 practices to be *Largely Implemented* or *Fully Implemented* based on implementation of a similar CMMC requirement.

## Threat and Vulnerability Management (THREAT)

| C2M2 Practice | | CMMC Requirement | |
|---|---|---|---|
| THREAT-1f | Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events | RA.L2-3.11.2 | Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. |

## Identity and Access Management (ACCESS)

| C2M2 Practice | | CMMC Requirement | |
|---|---|---|---|
| ACCESS-1a | Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities) | IA.L2-3.5.1 | Identify information system users, processes acting on behalf of users, or devices. |
| ACCESS-2a | Logical access controls are implemented, at least in an ad hoc manner | IA.L2-3.5.2 | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. |
| ACCESS-3c | Physical access logs are maintained, at least in an ad hoc manner | PE.L2-3.10.4 | Maintain audit logs of physical access. |

## Cybersecurity Architecture (ARCHITECTURE)

| C2M2 Practice | | CMMC Requirement | |
|---|---|---|---|
| ARCHITECTURE-3g | The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives) | MP.L2-3.8.7 | Control the use of removable media on system components. |
| ARCHITECTURE-5e | Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls | SC.L2-3.13.10 | Establish and manage cryptographic keys for cryptography employed in organizational systems. |

# APPENDIX C: REFERENCES


[C2M2 V2.1 Model Document]

US Department of Energy. 2022. Cybersecurity Capability Maturity Model, Version 2.1. Retrieved June 28, 2022, from https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[C2M2 V2.1 Self-Evaluation Guide]

US Department of Energy. 2022. Self-Evaluation Guide, Companion Document to C2M2 Version 2.1. Retrieved June 28, 2022, from https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[CMMC Level 2 Assessment Guide]

Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, & Futures, Inc. 2021. CMMC Assessment Guide, Level 2. Version 2.0. Retrieved February 7, 2022, from https://dodcio.defense.gov/CMMC/Documentation/

[CMMC Model]

Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, & Futures, Inc. 2020. Cybersecurity Maturity Model Certification (CMMC) Model Overview. Retrieved February 7, 2022, from https://dodcio.defense.gov/CMMC/Documentation/

[CMMC Level 2 Scoping Guidance]

Carnegie Mellon University, The Johns Hopkins University Applied Physics Laboratory LLC, & Futures, Inc. 2021. *CMMC Assessment Scope, Level 2*. Version 2.0 Retrieved February 7, 2022, from: https://dodcio.defense.gov/CMMC/Documentation/

[NIST SP 800-171]

Ross R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. 2020. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (NIST Special Publication 800-171 Revision 2). Retrieved February 7, 2022, from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

# APPENDIX D: ACRONYMS

| Acronym | Definition |
|---|---|
| C2M2 | Cybersecurity Capability Maturity Model |
| C3PAO | CMMC Third Party Assessment Organization |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CMMC | Cybersecurity Maturity Model Certification |
| CMVP | Cryptographic Module Validation Program |
| CSP | cloud service providers |
| CUI | controlled unclassified information |
| CVE | common vulnerabilities and exposures |
| DFARS | Defense Federal Acquisition Regulation Supplement |
| DIB | defense industrial base |
| DIBCAC | DIB Cybersecurity Assessment Center |
| DoD | Department of Defense |
| DOE | Department of Energy |
| EDR | endpoint detection and response |
| FAR | Federal Acquisition Regulation |
| FCI | federal contract information |
| FIPS | Federal Information Processing Standards |
| IDS | intrusion detection system |
| IoT | internet of things |
| IT | information technology |
| MDM | mobile device management |
| MIL | maturity indicator level |
| NIST | National Institute of Standards and Technology |
| OT | operations technology |
| POA&M | plan of action and milestones |
| RPO | recovery point objective |
| RTO | recovery time objective |
| SIEM | security information and event management |
| SLA | service level agreement |
| SME | subject matter expert |
| SPRS | Supplier Performance Risk System |
| SSP | System Security Plan |
| STIG | security technical implementation guide |
| US-CERT | United States Computer Emergency Readiness Team |

| Acronym | Definition |
|---|---|
| VOIP | voice over internet protocol |
| VPN | virtual private network |
| XDR | extended detection and response |

This material is based upon work funded and supported by the Department of Energy 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 sponsored by the United States Department of Defense.



DM22-0345