C2M2 | Cybersecurity Capability Maturity Model

Cybersecurity Capability Maturity Model (C2M2) – Cybersecurity Maturity Model Certification (CMMC) Supplemental Guidance

DRAFT

For Working Group Review

U.S. DEPARTMENT OF ENERGY
OFFICE OF
Cybersecurity, Energy Security, and Emergency Response

TABLE OF CONTENTS

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.

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

DM22-0345

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	**Kaitlin Brennan**
Southern Company	Edison Electric Institute (EEI)

Subgroup Members and Contributors

TABLE TO BE COMPLETED BEFORE PUBLISHING

Member, Organization	Member, Organization	Member, Organization

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 be used to:

- strengthen organizations' cybersecurity capabilities
- enable organizations to 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 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 private- and public-sector experts and representatives of asset owners and operators within the electricity subsector. The initiative used the National Infrastructure Protection Plan framework as a public-private partnership mechanism to support the development of the model.

The Cybersecurity Maturity Model Certification (CMMC) is the Department of Defense (DoD) program designed to strengthen cyber resiliency throughout the Defense Industrial Base (DIB); establish common assessment criteria; and put contractual compliance standards within DoD procurements.

CMMC 2.0, released in November 2021, is the current version of the model and is derived largely from two documents:

- *NIST SP800-171 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*.

As of this writing, CMMC is in the process of FAR and DFARS rulemaking, which will occur 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 – Foundational.** Focused on protecting Federal Contract Information (FCI), Level 1 has 17 basic requirements listed in the FAR and detailed in SP 800-171. Contractors will self-attest to compliance at least annually. Third party assessments will not be available.

- **Level 2** – **Advanced.** Level 2 includes all 110 requirements in SP 800-171 and is focused on protecting Controlled Unclassified Information (CUI). Level 2 certifications will be available from third-party assessors and organizations. The nature of the CUI may require contractors to achieve a L2 certification or may let them self-attest their compliance. The requirement for certification will be contract specific.

- **Level 3 – Expert.** Level 3 adds additional controls from 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 L3 certification must already possess a L2 certification.

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

- **DFARS 252.205-7012.** This clause has been in effect since 2017. It requires organizations to complete a self-assessment against 800-171, then develop a System Security Plan (SSP) and a plan of actions and milestones (POAM) based on the organization's people, processes, policy, and technology in use.

- **DFARS 252.205-7019/7020.** These clauses were introduced in November of 2020. They require that the SSP and POAM developed in accordance with DFARS 252.205-7012 are scored against a DoD-published methodology. The score, along with an estimated closure date of all POAM items (i.e., a perfect score) need to be loaded into the Supplier Performance Risk System (SPRS). Scores can be developed through self-assessments or are the result of assessments performed by the DIB Cybersecurity Assessment Center (DIBCAC).

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 POAM items to be closed within 180 days. Currently a POAM can be open indefinitely.

- Under CMMC, some practices must be fully implemented and cannot be included on a POAM. Currently there are no limits on POAM items.

- Although POAMs will be permitted, a minimum passing score for CMMC is expect.

- C3PAOs and certified assessors will perform CMMC L2 certifications. The government will conduct 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 it is also applies to organizations seeking Level 1 certification.

Caution to Readers

This guide serves solely as supplemental guidance in interpreting the overlap and applicability of C2M2, NIST 800-171, and CMMC. This is only guidance, C2M2 does not have reciprocity with CMMC. Therefore, C2M2 results cannot be used in place of a CMMC self-assessment or certification. However, much of the effort needed to implement C2M2 applies to meeting both DoD's current requirements as well as CMMC.

2. CORE CONCEPTS

This chapter describes several core concepts that are important for understanding the relationship between C2M2 and CMMC and for properly using this guidance document.

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	Required contract requirement for defense contractors
Structure	Practices organized by domains	Practices 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	Measures the institutionalization of cybersecurity activities	Policies and procedures may be required, but implementation is not measured

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 complimentary practices. By implementing the practices detailed in either model, organizations will improve their cybersecurity posture. Each model organizes cybersecurity activities into scaled levels. The higher the level, the more advanced or more complete the activities. There are also differences between the models with respect to their structure, the motivation behind the creation, and typical use.

There are structural similarities between the models, including 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 above, the DoD created CMMC to strengthen the cyber resilience of the DIB sector in response to targeting by malicious 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 improve their cybersecurity. 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. Its use is voluntary and is not for regulatory compliance.

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.

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 include:

- 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.

To properly prepare for a C2M2 self-evaluation or CMMC assessment, consider the differences between C2M2 and CMMC, such as the types of evaluations, scoping, and documentation requirements. This section provides a high-level overview of these considerations. Refer to *C2M2 Self-Evaluation Guide*, *CMMC Assessment Guides*, and *CMMC Scoping Guidance* for more information.

Note: This section compares C2M2 and CMMC. As of this writing, 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.

2.1.1 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 seek CMMC certification to meet DoD contractual requirements. Depending on the type of information DIB contractors are processing, storing, and transmitting, they may seek CMMC certification through a self-assessment or through a third-party- or government-led assessment. Based on currently planned CMMC requirements, contractors seeking Level 1, along with a subset of organizations seeking Level 2, may complete annual self-assessments if they support programs that do not involve information critical to national security. CMMC requires third-party assessments every three years for contractors who support programs that require Level 2 certification *and* involve information critical to national security.

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 practice. If an organization is subject to a third-party assessment, it should refer to the potential assessment methods and objects in the *CMMC Assessment Guide* for additional information regarding what or who an assessor may request to examine, interview, or test. Similar documentation is necessary even if an organization completes a self-assessment (e.g., SSP, network diagram, POAM). Regardless of the type of CMMC assessment, it is important for organizations to consider the individual assessment objectives of each CMMC practice. Organizations attest that they have met these assessment objectives; assessors evaluate them. At level 2, there are 320 assessment objectives in 110 practices.

2.1.2 Scoping

Prior to conducting a C2M2 self-evaluation workshop, the 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 the 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 the 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 practices. 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, restricted information systems, and test equipment. For an asset to be consider outside the scope of a CMMC assessment, it must be physically or logically separated from CUI assets.

2.1.3 Documentation

As mentioned above, 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 practice are detailed in *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 with evidence. 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 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 SP 800-171 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.

The CMMC model does not directly address the implementation of artifacts such as policies and procedures, but organizations should carefully review potential assessment objects in the *CMMC Assessment Guide* because these artifacts are included among those that may be examined. In addition, organizations should consider the tailoring criteria used in the development of NIST SP 800-171 Rev 2. Appendix E of SP 800-171 Rev 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 800-53 moderate baseline, which was the basis for the CUI-derived security requirements. Although CMMC may not explicitly require such artifacts as a system maintenance policy or a procedure for security awareness training, DIB contractors are expected to have them in place, communicate them, and maintained them.

3. APPLYING C2M2 TO CMMC

This section shows CMMC practices 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. The CMMC practice identifiers may be clicked to view more information on the noted CMMC practice in Appendix A.

THIS SECTION WILL BE UPDATED FOR C2M2 V2.1

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.	There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc	[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.	The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, operating system and firmware versions)	
	d.	Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function	
	e.	Prioritization criteria include consideration of assets within the function that may be leveraged to achieve a threat objective	
MIL3	f.	The IT and OT asset inventory is complete (the inventory includes all assets used for the delivery of 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	[CM.L2-3.4.1]
	h.	The IT and OT asset inventory is used to identify cyber risks, such as asset end of life or end of support and single points of failure	
	i.	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.L1-3.8.3]

2. Manage Information Asset Inventory

MIL1	a.	There is an inventory of information assets that are important to the delivery of the function (for example, SCADA set points and customer information); management of the inventory may be ad hoc	
MIL2	b.	The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective	
	c.	The information asset inventory includes attributes that support cybersecurity activities (for example, backup locations and frequencies, storage locations, cybersecurity requirements)	[PE.L2-3.10.6]
	d.	Inventoried information assets are categorized based on a defined scheme that includes importance to the delivery of the function	
	e.	Categorization criteria include consideration of assets within the function that may be leveraged to achieve a threat objective	
MIL3	f.	The information asset inventory is complete (the inventory includes all assets used for the delivery of 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	[CM.L2-3.4.1]]
	h.	The information asset inventory is used to identify cyber risks, such as risk of disclosure, risk of destruction, and risk of tampering	[AC.L1-3.1.22]
	i.	Information assets are sanitized or destroyed at the end of life using techniques appropriate to their cybersecurity requirements	

3. Manage 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	
MIL3	c.	The design of configuration baselines includes cybersecurity objectives	[SC.L2-3.13.9]
	d.	Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1e)	[CM.L2-3.4.9]
	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]
	f.	Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture	

4. Manage Changes to Assets

MIL1	a.	Changes to inventoried 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 inventoried assets are logged, at least in an ad hoc manner	
MIL2	c.	Changes to assets are tested prior to being deployed	
	d.	Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement)	[CM.L2-3.4.3] [MA.L2-3.7.1]
MIL3	e.	Changes to assets are tested for cybersecurity impact prior to being deployed	[CM.L2-3.4.4]
	f.	Change logs include information about modifications that impact the cybersecurity requirements of assets	

5. Management Activities

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.	Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel
	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.L1-3.14.1]
	b.	Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	[SI.L1-3.14.1]
	c.	Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner	[SI.L1-3.14.1]
	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.L1-3.14.1]
MIL2	e.	Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored (ASSET-1d)	
	f.	Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events	[RA.L2-3.11.2] [SI.L1-3.14.5]
	g.	Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly	[RA.L2-3.11.3]
	h.	Operational impact to the function is evaluated prior to deploying patches	
	i.	Information on any discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders	
MIL3	j.	Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function	
	k.	Identified vulnerabilities that pose ongoing risk to the function are referred to the risk management program for response	[RA.L2-3.11.3] [CA.L2-3.12.2]
	l.	Vulnerability monitoring activities include review and confirmation of actions taken in response to cybersecurity vulnerabilities where appropriate	[SI.L2-3.14.3]

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.	Cybersecurity threat information is gathered and interpreted for the function, at least in an ad hoc manner	
	c.	Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner	
MIL2	d.	A threat profile for the function is established (for example, characterization of potential threat actors, motives, intent, capabilities, and targets)	
	e.	Threat information sources that collectively address all components of the threat profile are prioritized and monitored	
	f.	Identified threats are analyzed and prioritized and are addressed accordingly	[SI.L2-3.14.3]
	g.	Threat information is exchanged with stakeholders (for example, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs], internal entities) based on risk to critical infrastructure	
MIL3	h.	The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events	
	i.	Threats that pose ongoing risk to the function are referred to the risk management program for action	
	j.	Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3h)	
	k.	Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action	

3 Management Activities

MIL1	No practice at MIL1	
MIL2	a.	Documented procedures are established, followed, and maintained for activities in the THREAT domain
	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.	Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel
	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 to support the organization’s cybersecurity program strategy (PROGRAM-1b) and enterprise architecture	
	c.	Information from RISK domain activities is communicated to relevant stakeholders	
	d.	Governance for the cyber risk management program is established and maintained	
MIL3	e.	A cyber risk management program is established and maintained to implement and perform activities in the RISK domain in alignment with the organization’s mission and objectives	
	f.	The cyber risk strategy and program activities are coordinated with the organization’s enterprise-wide risk management strategy and program	

2. Identify Cyber Risk

MIL1	a.	Cyber risks are identified, at least in an ad hoc manner	
MIL2	b.	Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level	
	c.	Cyber risk identification leverages multiple risk identification techniques and information sources	[RA.L2-3.11.1]
	d.	Stakeholders from appropriate operations and business areas participate in the identification of cyber risks	
	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	[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 new or unmitigated vulnerabilities)	

2. Identify Cyber Risk (continued)

MIL3	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.	Conformance gaps between as built systems and networks and the cybersecurity architecture are used to update cyber risks and identify new risks (ARCHITECTURE-1h)
	m.	Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interconnected 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 risk categories and cyber risks (for example, impact, likelihood, susceptibility, risk tolerance)
	c.	A defined method is used to estimate impact for higher priority cyber risk categories and cyber risks (for example, comparison to actual events, risk quantification)
	d.	Defined methods are used to analyze higher priority cyber risk categories and 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 support the analysis of higher priority cyber risk categories and cyber risks
	f.	Cyber risk categories and cyber risks are retired 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 and external events

4. Respond to Cyber Risk

MIL1	a.	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risk categories and cyber risks, at least in an ad hoc manner	[AC.L1-3.1.22] [RA.L2-3.11.3] [CA.L2-3.12.2] [SI.L2-3.14.3]
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

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.	Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel
	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 and Maintain Identities

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.L1-3.5.1]
	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	
	c.	Identities are deprovisioned, at least in an ad hoc manner, when no longer required	
MIL2	d.	Identity repositories are reviewed and updated to ensure accuracy, periodically and according to defined triggers, such as system changes and changes to organizational structure	
	e.	Identities are deprovisioned within organization-defined time thresholds when no longer required	[IA.L2-3.5.6] [MA.L2-3.7.5]
	f.	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)	[AC.L2-3.1.7] [AC.L2-3.1.15] [AU.L2-3.3.9] [IA.L2-3.5.3] [MA.L2-3.7.5]

2. Control Logical Access

MIL1	a.	Logical access controls are implemented, at least in an ad hoc manner	[AC.L1-3.1.1] [AC.L1-3.1.2] [AC.L2-3.1.17] [AC.L2-3.1.18] [CM.L2-3.4.5] [IA.L1-3.5.2] [MA.L2-3.7.2]
	b.	Logical access is revoked when no longer needed, at least in an ad hoc manner	[PS.L2-3.9.2]
MIL2	c.	Logical access requirements are determined (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.L1-3.1.1] [AC.L1-3.1.2] [AC.L2-3.1.7] [AC.L2-3.1.15] [AC.L2-3.1.16] [CM.L2-3.4.5]

2. Control Logical Access (continued)

MIL2	h.	Logical access requirements incorporate the principle of least privilege	[AC.L2-3.1.5]
	i.	Logical access requirements incorporate separation of duties	[AC.L2-3.1.4]
	j.	Logical access requests are reviewed and approved by the asset owner	[AC.L2-3.1.15] [AU.L2-3.3.9]
	k.	Logical access that poses higher risk to the function receives additional scrutiny and monitoring	[AC.L2-3.1.7] [AU.L2-3.3.8] [AU.L2-3.3.9]
MIL3	l.	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	
	m.	Anomalous access attempts are monitored as indicators of cybersecurity events	[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.L1-3.10.1] [PE.L2-3.10.2] [PE.L1-3.10.5]
	b.	Physical access is revoked when no longer needed, at least in an ad hoc manner	[MP.L2-3.8.2] [PE.L1-3.10.5]
	c.	Physical access logs are maintained, at least in an ad hoc manner	[MP.L2-3.8.2] [PE.L1-3.10.4]
MIL2	d.	Physical access requirements are determined (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.L1-3.10.1] [PE.L1-3.10.5] [PE.L2-3.10.6]
	e.	Physical access requirements incorporate the principle of least privilege	
	f.	Physical access requests are reviewed and approved by the asset owner	
	g.	Physical access that poses higher risk to the function receives additional scrutiny and monitoring	[PE.L1-3.10.3]
MIL3	h.	Physical access privileges are reviewed and updated	[PE.L1-3.10.5]
	i.	Physical access is monitored to identify potential cybersecurity events	[MA.L2-3.7.6] [PE.L2-3.10.2]

4. Management Activities

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. Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities
	e. Responsibility, accountability, and authority for the performance of activities in the ACCESS domain are assigned to personnel
	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 important to the delivery of the function, at least in an ad hoc manner (ASSET-1a, ASSET-2a)	[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 assets important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective (ASSET-1a, ASSET-2a)	[AC.L2-3.1.7] [AU.L2-3.3.1] [AU.L2-3.3.2] [AU.L2-3.3.3]
	d.	Log data are being aggregated within the function	
MIL3	e.	More rigorous logging is performed for higher priority assets (ASSET-1d)	

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]
	b.	IT and OT environments are monitored for anomalous activity that may indicate a cybersecurity event, at least in an ad hoc manner	[AU.L2-3.3.5]
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.L2-3.14.3] [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.L2-3.14.3] [SI.L2-3.14.6]
	f.	Monitoring activities are aligned with the threat profile (THREAT-2d)	

2. Perform Monitoring (continued)

MIL3	g.	More rigorous monitoring is performed for higher priority assets (ASSET-1d)	[AC.L2-3.1.18]
	h.	Continuous monitoring is performed across IT and OT environments to identify anomalous activity	[AC.L2-3.1.11] [SI.L2-3.14.7]
	i.	Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity	
	j.	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.	Monitoring data are aggregated and analyzed to provide near-real-time understanding of the cybersecurity state of the function	[AU.L2-3.3.5] [AU.L2-3.3.6]
	f.	Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness	
	g.	Procedures are in place to analyze received cybersecurity information in support of situational awareness	
	h.	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 (THREAT-2j, RESPONSE-3k)	

4. Management Activities

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.	Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel
	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 logged, at least in an ad hoc manner	
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 logged based on the established criteria	
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 (RISK-2a) and the organization's threat profile (THREAT-2d)	
	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	
	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 logged and tracked to closure	[IR.L2-3.6.2]
	g.	Cybersecurity stakeholders (for example, government, connected organizations, vendors, sector organizations, regulators, and internal entities) are identified and notified of events and incidents based on situational awareness reporting requirements (SITUATION-3d)	[IR.L2-3.6.2]

2. Analyze Cybersecurity Events and Declare Incidents (continued)

MIL3	h.	Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b)	
	i.	Cybersecurity incidents are correlated to support the discovery of patterns, trends, and other common features	

3. Respond to Cybersecurity Events and Incidents

MIL1	a.	Cybersecurity event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner	
	b.	Responses to cybersecurity events and 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	
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 event and incident response is executed according to defined plans and procedures	
	f.	Cybersecurity event and incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events	[IR.L2-3.6.3]
	g.	Cybersecurity event and incident lessons-learned activities are performed and corrective actions are taken, including updates to the incident response plan	
MIL3	h.	Cybersecurity event and incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan	
	i.	Cybersecurity event and incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation	
	j.	Cybersecurity event and incident response personnel participate in joint cybersecurity exercises with other organizations	
	k.	Cybersecurity event and incident responses leverage and trigger predefined states of operation (SITUATION-3h)	

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.	An analysis of the impacts from potential cybersecurity events informs the development of continuity plans	
	e.	The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans	

4. Address Cybersecurity in Continuity of Operations (continued)

MIL 2	f.	Continuity plans address IT, OT, and information assets important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets (ASSET-1a, ASSET-2a)	
	g.	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]
	h.	Data backups are protected with at least the same controls as source data	[MP.L2-3.8.9]
	i.	Data backups are logically or physically separated from source data	
	j.	Spares for selected IT and OT assets are available	
	k.	Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets important to the delivery of the function are incorporated into continuity plans (ASSET-1a, ASSET-2a)	
	l.	Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel	
MIL 3	m.	Continuity plans are aligned with identified risks (RISK-2a) and the organization’s threat profile (THREAT-2d) to ensure coverage of identified risk categories and threats	
	n.	Continuity plan exercises address higher priority risks (RISK-3a)	
	o.	The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly	
	p.	Cybersecurity incident content within continuity plans is periodically reviewed and updated	
	q.	Continuity plans are periodically reviewed and updated	

5. Management Activities

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.	Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities	
	e.	Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel	
	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 important to the delivery of the function are identified, at least in an ad hoc manner	[MA.L2-3.7.2]
MIL2	c.	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)	
	d.	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	e.	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 are formalized in agreements with suppliers and other third parties where applicable	

2. Manage Third-Party Risk (continued)

MIL2	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 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.	Acceptance testing of procured assets includes testing for cybersecurity requirements

3. Management Activities

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.	Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel
	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. 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

2. 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.	Training, recruiting, and retention efforts are aligned to address identified workforce gaps	[AT.L2-3.2.2]
	d.	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function	[AT.L2-3.2.1] [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	

3. 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 periodically for positions that have access to the assets required for delivery of the function	[PS.L2-3.9.1]
	d.	Personnel transfer procedures address cybersecurity	[PS.L2-3.9.2]
	e.	Users are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets	[AC.L1-3.1.22] [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	

4. Increase Cybersecurity Awareness

MIL1	a.	Cybersecurity awareness activities occur, at least in an ad hoc manner	[AT.L2-3.2.1] [AT.L2-3.2.3] [SI.L2-3.14.7]
MIL2	b.	Objectives for cybersecurity awareness activities are established and maintained	
	c.	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2d)	[AT.L2-3.2.3]
MIL3	d.	Cybersecurity awareness activities are aligned with the predefined states of operation (SITUATION-3h)	
	e.	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	

5. Management Activities

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.	Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel
	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 to support 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 board) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process	
	e.	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]
	f.	Cybersecurity controls are selected and implemented to meet cybersecurity requirements	[SC.L2-3.13.2]
MIL3	g.	The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program	
	h.	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]
	i.	The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2d)	
	j.	The cybersecurity architecture addresses predefined states of operation (SITUATION-3h)	

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

MIL1	a.	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	[SC.L1-3.13.5]
MIL2	b.	Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements (ASSET-1a, ASSET-2a)	[SC.L1-3.13.1] [SC.L2-3.13.3]
	c.	Network protections incorporate the principles of least privilege and least functionality	
	d.	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)	[SC.L2-3.13.9]
	e.	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])	[AC.L1-3.1.20] [SC.L1-3.13.1] [SC.L2-3.13.6] [SC.L2-3.13.7] [SC.L2-3.13.14] [SC.L2-3.13.15] [SI.L1-3.14.2]
	f.	Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techiniques, IP address blocking)	[SC.L1-3.13.1] [SI.L1-3.14.2]
MIL3	g.	All assets are segmented into distinct security zones based on cybersecurity requirements	[SC.L2-3.13.3]
	h.	Isolated networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication	
	i.	OT systems are operationally independent from IT systems so that OT operations are unimpeded by an outage of IT systems	
	j.	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)	[AC.L2-3.1.12] [AC.L2-3.1.13] [AC.L2-3.1.14] [SC.L1-3.13.1] [SC.L2-3.13.14] [SC.L2-3.13.15]
	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]
	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.	Cybersecurity controls are implemented for assets important to the delivery of the function, at least in an ad hoc manner	[SC.L2-3.13.9]
MIL2	b.	More rigorous cybersecurity controls are implemented for higher priority assets (ASSET-1d)	
	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 implemented as part of the asset deployment process where feasible	[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] [SI.L1-3.14.2]
	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, including physical access controls, are implemented for all assets used for the delivery of the function (ASSET-1f) either at the asset level or as compensating controls where asset-level controls are not feasible	
MIL3	i.	Configuration of and changes to firmware are controlled throughout the asset lifecycle	
	j.	Controls are implemented to prevent the execution of unauthorized code	[SC.L2-3.13.13] [SI.L1-3.14.2]

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 (ASSET-1d) is developed using secure software development practices	[SC.L2-3.13.2]
	b.	The selection of procured software for deployment on higher priority assets (ASSET-1d) includes consideration of the vendor’s secure software development practices	
	c.	Secure software configurations are required as part of the software deployment process	[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	[SC.L2-3.13.2]

4. Implement Software Security as an Element of the Cybersecurity Architecture (continued)

MIL3	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 (ASSET-2d)	
	c.	All data in transit is protected for selected data categories (ASSET-2d)	
	d.	Cryptographic controls are implemented for data at rest and data in transit for selected data categories (ASSET-2d)	[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	
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	
	h.	The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data	

6. Management Activities

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.	Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities	
	e.	Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel	
	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 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, NIST guidelines, Payment Card Industry Data Security Standard, ISO, CMMC, and the California Consumer Privacy Act)
MIL3	h.	The cybersecurity program strategy is updated to reflect business changes, changes in the operating environment, and changes in the threat profile (THREAT-2d)

2. Sponsor Cybersecurity Program

MIL1	a.	Resources (people, funding, and tools) are provided, at least in an ad hoc manner, to establish the cybersecurity program
	b.	Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner
MIL2	c.	The cybersecurity program is established according to the cybersecurity program strategy
	d.	Adequate resources (people, funding, and tools) are provided to operate a cybersecurity program aligned with the program strategy
	e.	Senior management sponsorship for the cybersecurity program is visible and active
	f.	Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies
	g.	Responsibility for the cybersecurity program is assigned to a role with sufficient authority
	h.	Stakeholders for cybersecurity program management activities are identified and involved
MIL3	i.	Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy
	j.	Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes
	k.	The cybersecurity program addresses and enables the achievement of regulatory compliance, as appropriate
	l.	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

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.	Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities
	e.	Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel
	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 used C2M2 to evaluate their cybersecurity capabilities or may be used in conjunction with the completion of a C2M2 evaluation. Levels 1 and 2 CMMC practices are detailed in this section and are arranged in the same order as the practices documented in the Level 2 *CMMC Assessment Guide* that has been released by the Department of Defense.

ACCESS CONTROL

AC.L1-3.1.1

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 SP800-171 Reference: 3.1.1

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
ACCESS-2c	Logical access requirements are determined (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-2a and ACCESS-2c would likely provide a capability similar to AC.L1-3.1.1. To satisfy the assessment objectives of AC.L1-3.1.1, the 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 will also help to enable the organization to audit the actions of users, processes acting on behalf of authorized users, and devices.

Before access is granted to an information system, the organization should use a defined method to grant authorization. For example, a user wishes to access an internal datastore that is used to store restricted information but must first request authorization to access the datastore. This may be accomplished through a help desk process that verifies with a resource owner that a user is authorized to access the resource. After receiving approval, the help desk would grant the user access.

AC.L1-3.1.2

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 SP800-171 Reference: 3.1.2

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
ACCESS-2c	Logical access requirements are determined (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-2a and ACCESS-2c would likely provide a capability similar to AC.L1-3.1.2. Access to resources like applications and data should be limited to the resources necessary for a user to fulfill their job responsibilities. The defined access requirements should be used to limit access to resources, such as restricting a user to only have read access to a shared folder, while having 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 access is granted based on user job role. An access control list is implemented that only allows users from a customer support team to access the information.

AC.L1-3.1.20

CMMC Short Name: External Connections

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

NIST SP800-171 Reference: 3.1.20

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])

Discussion:

Organizations that have Fully Implemented or Largely Implemented ARCHITECTURE-2e will likely have a similar capability to AC.L1-3.1.20. It is important to note that “external information systems” will be dependent upon the CMMC Assessment Scope. These may be systems that are outside of the organization’s network or could be within the organization’s network if a the CMMC Assessment Scope is a limited portion of the organization’s network (e.g., enclave, lab).

The 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 VPN may be implemented that requires a vendor to use unique credentials. The organization may also consider implementing policies that define acceptable use of external systems.

AC.L1-3.1.22

CMMC Short Name: Control Public Information

Control information posted or processed on publicly accessible information systems.

NIST SP800-171 Reference: 3.1.22

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ASSET-2h	The information asset inventory is used to identify cyber risks, such as risk of disclosure, risk of destruction, and risk of tampering
RISK-4a	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risk categories and cyber risks, at least in an ad hoc manner
WORKFORCE-3e	Users 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 ASSET-2h, RISK-4a, and WORKFORCE-3e may have a similar capability to AC.L1-3.1.22. This CMMC practice does have specific requirements regarding FCI that organizations should consider in implementing these practices.

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

AC.L2-3.1.3

CMMC Short Name: Control CUI Flow

Control the flow of CUI in accordance with approved authorizations.

NIST SP800-171 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 (ASSET-2d)
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 would likely help an organization to implement the requirements needed to meet AC.L2-3.1.3, but the organization must consider CUI-specific requirements. To meet the assessment objectives of AC.L2-3.1.3, the organization must understand how information flows throughout the network, and more specifically, for 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 will help the organization build network protections that can control the flow of CUI throughout the network.

An organization has a policy that defines 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 the 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 SP800-171 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 separation of duties

Discussion:

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

Separate identities for all users will help organizations to meet this practice as it will give them the ability to separate user access to specific system functions or information. 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 SP800-171 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 similar capability to the requirements of AC.L2-3.1.5. The organization should carefully consider if 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 for roles that have an operational need to perform security functions. For example, a network administrator may have the responsibility of managing firewall rules. The organization could restrict access to the firewall configuration to a dedicated privileged account that is 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 SP800-171 Reference: 3.1.6

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

New MIL2 ACCESS-1 practice (proposed)

Discussion:

An organization that has Fully Implemented or Largely Implemented ACCES-1X will likely have a similar capability to AC.L2-3.1.6. To achieve this practice, the organization should ensure that it has considered and defined which functions should only be completed by privileged accounts and which should be completed by standard accounts. 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 such as changing system configuration settings or adding an application to an allowlist, that requires privileged access. A separate account should be provisioned for these users that is intended to be used specifically for these job responsibilities.

Policies, procedures, and training for users that are granted privileged access should include restrictions on the use of privileged accounts for job responsibilities that do not require the use of a privileged account. An organization should identify activities that require privileged access, such as changing detection rules for an intrusion detection system (IDS). A network security engineer that has responsibility for maintaining the detection rules would be issued a separate administrative account that would be used for updating the detection rules, but not for nonsecurity functions like 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 SP800-171 Reference: 3.1.7

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ACCESS-1f	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)
ACCESS-2c	Logical access requirements are determined (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 that poses higher risk to the function receives additional scrutiny and monitoring
SITUATION-1a	Logging is occurring for assets important to the delivery of the function, at least in an ad hoc manner (ASSET-1a, ASSET-2a)
SITUATION-1c	Logging requirements are established and maintained for assets important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective (ASSET-1a, ASSET-2a)

Discussion:

An organization that has Fully Implemented or Largely Implemented ACCESS-1f, ACCESS-2c, ACCESS-2g, SITUATION-1a, and SITUATION-1c will likely have a similar capability to AC.L2-3.1.7. Achievement of this practice requires the organization to define privileged functions, clearly distinguish between privileged and non-privileged account, limit the execution of privileged functions, and log the execution of privileged functions.

Privileged functions should be identified and documented by the organization. This will enable the organization to build security controls around these functions to limit execution by standard users and implement logging to identify the execution of these 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 could be achieved by granting these additional permissions to a separate administrative user account. Regardless of the type of account or permissions granted to an account, the execution of any privileged functions should be logged. Logging all privileged functions will enable the identification of non-privileged users attempting to execute privileged functions or incorrect allocation of permissions that could allow misuse of privileged functions.

AC.L2-3.1.8

CMMC Short Name: Unsuccessful Logon Attempts

Limit unsuccessful logon attempts.

NIST SP800-171 Reference: 3.1.8

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This practice is related to practices in the second objective of ACCESS, Control Logical Access, but does not have a direct relationship.

Limiting unsuccessful logon attempts will help to mitigate attacks, such as a brute force attack against 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 all in-scope assets. Methods to limit unsuccessful logon attempts should be identified and implemented at all authentication points. These methods may be built into software like setting an account lockout threshold policy setting in Microsoft Windows.

AC.L2-3.1.9

CMMC Short Name: Privacy & Security Notices

Provide privacy and security notices consistent with applicable CUI rules.

NIST SP800-171 Reference: 3.1.9

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

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

Organizations may have an existing system use notification that notifies users of acceptable use and system use monitoring. A similar functionality could be implemented that also identifies CUI-specific requirements and requires a user to agree 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 may 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 SP800-171 Reference: 3.1.10

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This practice does not have a direction relationship with C2M2. Implementation of this practice will help 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 functionality to configure a system to lock after a period of inactivity and display a lock screen that obscures the information on the screen. The organization should first define a period of inactivity that would trigger the operating system to lock a session and 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 SP800-171 Reference: 3.1.11

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

SITUATION-2h	Continuous monitoring is performed across IT and OT environments to identify anomalous activity

Discussion:

Fully Implementing or Largely Implementing SITUATION-2h may provide some of the same capability as AC.L2-3.1.11, but organizations should carefully review the specific requirements detailed in the assessment objectives. This CMMC practice requires that user-initiated logical sessions be automatically terminated if defined conditions are met. These conditions may be configured based on criteria like a period of time or other defined conditions, such as accessing application functionality that has not been granted to a user.

An organization may use an application like 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 time period to prevent misuse of the session by an attacker. Monitoring of user activity could also trigger termination of a session, such as accessing information in a database if the 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 SP800-171 Reference: 3.1.12

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2j	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2j would likely help an organization to meet AC.L2-3.1.12, but should carefully review the specific requirements detailed in the assessment objectives. While this practice requires the control and monitoring of remote access, documented policy on remote access is equally as important.

Organizations should carefully consider the risk that implementing remote access may introduce, particularly for those that handle CUI. Remote access that meets organizational thresholds should be expressed in policy. This policy could then 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, the organization may state that systems should be configured to only use 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 SP800-171 Reference: 3.1.13

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2j	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)

Discussion:

It is likely that Fully Implementing or Largely Implementing ARCHITECTURE-2j would provide the same capability as described in AC.L2-3.1.13, but organizations should carefully consider if their implementation of remote access meets the specific requirements of this CMMC practice.

If not properly secured, remote access can serve as a threat vector for attackers. Encrypting remote network access provides protection for information that is being transmitted between two locations, such as between home and corporate networks or 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 that will be used to protect CUI. To meet this CMMC practice, it is required that the remote access solution uses FIPS-validated cryptography. The cryptographic module used to implement the algorithm must be validated under FIPS 140.

AC.L2-3.1.14

CMMC Short Name: Remote Access Routing

Route remote access via managed access control points.

NIST SP800-171 Reference: 3.1.14

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-2j	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)

Discussion:

It is likely that Fully Implementing or Largely Implementing ARCHITECTURE-2j would provide a similar capability as described in AC.L2-3.1.14, but organizations should carefully consider if their implementation of remote access meets the specific requirements of this CMMC practice.

One method organizations may employ to reduce the risk of remote access solutions is reducing 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 they have identified and documented managed remote access control points. Monitoring of network traffic can help the organization to 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 SP800-171 Reference: 3.1.15

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ACCESS-1f	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)
ACCESS-2c	Logical access requirements are determined (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-1f, ACCESS-2c, and ACCESS-2f would likely provide a similar capability to the requirements of this CMMC practice. Additional consideration should be given to remote access that allows the execution of privileged commands or accessing security-relevant information.

The organization may grant some users the necessary permissions 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 still be permitted to execute these commands remotely. The privileged commands and security-relevant information that users should be 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 SP800-171 Reference: 3.1.16

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ASSET-1a	There is an inventory of IT and OT assets that are important to the delivery of the function; management of the inventory may be ad hoc
ACCESS-2c	Logical access requirements are determined (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:

An organization that has Fully Implemented or Largely Implemented ASSET-1a, ACCESS-2c, and ARCHITECTURE-2k would likely have a similar capability to AC.L2-3.1.16. To meet this CMMC practice, the organization should have an inventory of all authorized wireless access points, along with defining and enforcing 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, the organization should define requirements that must be met prior to authorizing a wireless connection, such as device configuration requirements. Wireless access should require users to authenticate similar to the requirements that are in place for wired connections.

AC.L2-3.1.17

CMMC Short Name: Wireless Access Protection

Protect wireless access using authentication and encryption.

NIST SP800-171 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 (ASSET-2d)

Discussion:

The requirements for AC.L2-3.1.17 would likely be met if an organization has Fully Implemented or Largely Implemented both ACCESS-2a and ARCHITECUTRE-5d. Organizations should ensure that FIPS-validated cryptography is used for encrypting wireless communications as this is a requirement when CUI is transmitted or stored outside the protected environment of the covered contractor information system.

Implementation of this CMMC practice may vary depending on the size of the organization. Authentication may be via 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. Modules that have been validated are listed on the NIST Cryptographic Module Validation Program (CMVP) website.

AC.L2-3.1.18

CMMC Short Name: Mobile Device Connection

Control connection of mobile devices.

NIST SP800-171 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 important to the delivery of the function, at least in an ad hoc manner (ASSET-1a, ASSET-2a)
SITUATION-2g	More rigorous monitoring is performed for higher priority assets (ASSET-1d)

Discussion:

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

Organizations should carefully balance the 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 the organization is able to adequately monitor and log connections from these devices. These devices should only be permitted to connect to the organization’s network once approved and authorized. A mobile device management (MDM) solution may help an organization to identify and monitor these devices.

AC.L2-3.1.19

CMMC Short Name: Encrypt CUI on Mobile

Encrypt CUI on mobile devices and mobile computing platforms.

NIST SP800-171 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 (ASSET-2d)

Discussion:

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

Mobile devices like smartphones that are permitted to access CUI introduce unique challenges since they could be more easily lost or stolen than other organizational assets. Implementing encryption to prevent disclosure of CUI or other sensitive information will help to mitigate this risk. Like other CMMC practices that require the use of cryptography, this practice requires that the cryptography used is FIPS-validated. Organizations may 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 SP800-171 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 similar capability as AC.L2-3.1.21, but this practice has CUI-specific requirements that organizations would 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 practice will vary based upon the scope and size of the organization. For example, a small organization that has an enterprise-level scope may determine it is sufficient to designate and label specific removeable media as permitted to store CUI and administratively limit the use of these devices outside the organization. A larger organization may take a different approach, including technical controls that only allow 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 SP800-171 Reference: 3.2.1

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

WORKFORCE-2d	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function
WORKFORCE-3e	Users are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets
WORKFORCE-4a	Cybersecurity awareness activities occur, at least in an ad hoc manner

Discussion:

AT.L2-3.2.1 has requirements that may be met by Fully Implementing or Largely Implementing WORKFORCE-2d, WORKFORCE-3e, and WORKFORCE-4a. But organizations should consider the CUI-specific requirements of this CMMC practice.

Organizations should ensure that individuals that are trusted with sensitive information, such as CUI, are made aware of their responsibilities for preventing the disclosure of such information. Similarly, individuals that have privileged access to systems and resources should be made aware of their increased responsibility and implications if this access is misused. This may be achieved through awareness training and regular communications. Employee responsibility for information and data security should be documented in policies. The organization should make employees aware of these 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 SP800-171 Reference: 3.2.2

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

WORKFORCE-2a	Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner
WORKFORCE-2c	Training, recruiting, and retention efforts are aligned to address identified workforce gaps
WORKFORCE-2d	Cybersecurity training is provided as a prerequisite to granting access to assets that support the delivery of the function

Discussion:

Fully Implementing or Largely Implementing WORKFORCE-2a, WORKFORCE-2c, and WORKFORCE-2d would likely provide a similar capability to AT.L2-3.2.2.

Staff with cybersecurity duties have unique responsibilities and organizations should document the roles and responsibilities necessary to properly secure sensitive information. Assigning cybersecurity-related duties, roles, and responsibilities ensures that there are not gaps between necessary requirements to secure information and actual implementation. It is also essential that the organization continually evaluates if staff responsible for cybersecurity-related duties have the necessary training to carry out their assigned responsibilities. Organizations may 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 SP800-171 Reference: 3.2.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

WORKFORCE-4a	Cybersecurity awareness activities occur, at least in an ad hoc manner
WORKFORCE-4c	Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2d)

Discussion:

Fully Implementing or Largely Implementing both WORKFORCE-4a and WORKFORCE-4c may provide a similar capability 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 as they stem from trusted individuals. These include both actions that cause intentional harm and unintentional actions that cause harm to the 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 these threats will reduce the potential impact to the 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 SP800-171 Reference: 3.3.1

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

SITUATION-1a	Logging is occurring for assets important to the delivery of the function, at least in an ad hoc manner (ASSET-1a, ASSET-2a)
SITUATION-1c	Logging requirements are established and maintained for assets important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective (ASSET-1a, ASSET-2a)

Discussion:

Fully Implementing or Largely Implementing SITUATION-1a and SITUATION-1c would likely provide a similar capability to AU.L2-3.3.1. Logging is commonly enabled on devices and logs are rarely reviewed until something breaks. While that may seem sufficient with regards to the health of physical devices, that approach will not raise your cyber resiliency and protect your organization.

Simply enabling logging on devices, systems, and user accounts is not sufficient to protect your environment, does not meet the intent of this practice, and would likely fail a third party audit. Irrespective of any compliance requirements, logging and monitoring are intended to provide an early tripwire to indicate 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 your current SITUATION practices with respect to CMMC are:

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

While not specifically called out, a SIEM solution is a cost effective way to collect the huge volumes of log data created, corollate events across multiple platforms, protect logs from tampering, and help you meet your retention requirements. They are especially valuable in triggering alerts of 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 you capture and review provided it provides enough detail to support monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity. Even if you never process CUI, logs from Security Protection Assets are critical to meeting the intent and requirements of this practice. Specialized Assets and Contractor Risk Managed Assets may not be assessed in the same way as other assets but the need to protect and monitor them still exists. See the CMMC Scoping Guides for more detail.

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 SP800-171 Reference: 3.3.2

DoD 800-171 Assessment Methodology Point Value: 3

Related C2M2 Practices

SITUATION-1c	Logging requirements are established and maintained for assets important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective (ASSET-1a, ASSET-2a)

Discussion:

Fully Implementing or Largely Implementing may provide similar capability to AU.L2-3.3.2, but organizations should ensure that the CMMC-specific requirements are reviewed. In the context of this CMMC practice, “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 will help make this practice achievable.

In addition to not sharing user accounts, capture as much information about the user performing a transaction on a system. This would include such things as user IDs, source and destination addresses, time stamps. Use multiple data points as well; user authentication data coupled with MFA logs increases the likelihood that a specific user performed the audited action. Ensure 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 SP800-171 Reference: 3.3.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

SITUATION-1c	Logging requirements are established and maintained for assets important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective (ASSET-1a, ASSET-2a)
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 and SITUATION-2c would 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. Ensure that your audit policies are up to date, are periodically reviewed and reflect changes in your infrastructure as well as the evolving threat landscape. In particular, ensure your retention policies reflect the fact that incidents are often not detected for weeks or months and that longer term storage of audit logs may be needed to provide the information to support an investigation.

Additionally, ensure the data collected is at the proper level and detail and the logs from the correct systems are being maintained. Update anytime there is a change to the security assets and/or major system changes occur. When using Cloud Service Providers (CSP), remember that 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 SP800-171 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 practice 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 [a]. Notifications (e.g., email, Short Message Service (SMS)) should be sent to the company's designated security personnel to immediately take 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 SP800-171 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	IT and OT environments are monitored for anomalous activity that may indicate a cybersecurity event, 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-3e	Monitoring data are aggregated and analyzed to provide 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-3e would 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 and large organizations will use some type of automated system that correlates log information from across the enterprise. Implementation of SITUATION-3d and SITUATION-3e cannot realistically be done without the use of an automated tool (i.e., a SIEM).

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

An automated SIEM (preferably managed) provides are a far greater level of accuracy in correlating events and identifying possible incidents and a much lower cost. Additionally, the practice is easier for an auditor to validate when the 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 SP800-171 Reference: 3.3.6

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

SITUATION-3e	Monitoring data are aggregated and analyzed to provide near-real-time understanding of the cybersecurity state of the function

Discussion:

Fully Implementing or Largely Implementing SITUATION-3e may provide some of the capability of AU.L2-3.3.6, but the specific requirements of this CMMC practice should be reviewed. Raw audit log data is difficult to review, analyze, and report because of the volume of data. 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 practice. The objective in both frameworks 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 in the case of CMMC, support forensic investigations. The tools you have 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 your systems. When configuring them, look at data retention settings. In many cases, possible intrusions and compromises are not detected for weeks or even months. Ensure your 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 SP800-171 Reference: 3.3.7

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This CMMC practice does not have a direct relationship with C2M2. 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. Be aware of what settings are used by default and ensure all your 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 SP800-171 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 would likely provide some of the capability of AU.L2-3.3.8, but the specific requirements of this CMMC practice should be reviewed. Access to audit logging tools and audit information would likely be considered higher risk to the function, but organizations should confirm if this is reflected in their logical access policies.

Assuming you have deployed an automated tool to capture, analyze, aggregate, and store your audit logs, you have probably met most of the requirement in CMMC. Your tool should pull the logs – from all sources – and store it in a way which prevents any 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 your 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 SP800-171 Reference: 3.3.9

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ACCESS-1f	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)
ACCESS-2f	Logical access requests are reviewed and approved by the asset owner
ACCESS-2g	Logical access that poses higher risk to the function receives additional scrutiny and monitoring

Discussion:

Fully Implementing or Largely Implementing ACCESS-1f, ACCESS-2f, and ACCESS-2g would likely provide similar capability to AU.L2-3.3.9, but additional require 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 you separate 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 you 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 SP800-171 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 used for the delivery of the function)
ASSET-1g	The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes
ASSET-2f	The information asset inventory is complete (the inventory includes all assets used for the delivery of the function)
ASSET-2g	The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes
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-1g, ASSET-2f, ASSET-2g, ASSET-3a, and ASSET-3e would likely provide a similar capability 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 the 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 SP800-171 Reference: 3.4.2

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

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-1h	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 implemented 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-3e, ARCHITECTURE-1c, ARCHITECTURE-1h, ARCHITECTURE-3e, and ARCHITECTURE-3f would likely provide a similar capability to CM.L2-3.4.2. When developing configuration baselines or other situations where an asset is put into service, organizations should consider if 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. Organizational should also consider if asset configurations meet the organization's security policies, compliance requirements, or other requirements around safety and reliability. In some instances, the default configuration of an asset may introduce additional risk to an organization through a vulnerability like an open port that a threat actor may leverage for 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 SP800-171 Reference: 3.4.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ASSET-4a	Changes to inventoried assets are evaluated and approved before being implemented, at least in an ad hoc manner
ASSET-4d	Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement)

Discussion:

Fully Implementing or Largely Implementing ASSET-4a and ASSET-4d would like provide a similar capability to CM.L2-3.4.3. A defined process to manage changes will enable the organization to more efficiently identify a change that has impacted 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 would likely include a workflow that would give 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 that were 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 SP800-171 Reference: 3.4.4

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

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

Discussion:

Fully Implementing or Largely Implementing ASSET-4e would likely provide the same capability as CM.L2-3.4.4. Changes may be tested prior to implementation for impact to 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 carefully plan the implementation of changes around scheduled downtime to prevent unintended impacts to production as the result of a change. Changes should also be thoroughly tested to identify any potential security issues that a change may introduce into the environment. Identification of these 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 SP800-171 Reference: 3.4.5

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
ACCESS-2c	Logical access requirements are determined (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 determined (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-2a, ACCESS-2c, ACCESS-3a, and ACCESS-3d would likely provide a similar capability to CM.L2-3.4.5. Controls to prevent unauthorized users from making changes to assets builds upon other configuration management practices to ensure that configurations can be maintained within organizational requirements.

Organizations should consider the logical and physical requirements that may need to be met to reduce the likelihood changes being performed by an unauthorized individual. These requirements may be defined and documented in an access control policy that is approved by appropriate organizational stakeholders. This policy could then be used to develop and implement controls that enforce access restrictions. These controls may include logical access controls like 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 SP800-171 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 would likely provide the same capability as CM.L2-3.4.6. In addition to CM.L2-3.4.2 that requires secure configurations, organizations should also consider if assets are being configured to provide the least functionality necessary.

It is important for organizations to carefully review configuration settings or functions that are enabled by default and determine which settings or functions 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. Organization should define system capabilities that are necessary to meet operational requirements and disable capabilities that do not meet those 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 SP800-171 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 would likely provide the same capability as CM.L2-3.4.7. In addition to CM.L2-3.4.2 that requires secure configurations, organizations should also consider if 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 and not 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 assets configured to meet these requirements. Various methods can be used to examine an asset to ensure it meets defined requirements, such as utilities built into the operating system or running 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 SP800-171 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

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-3d would like 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 that organizations consider the software that is necessary to meet operational requirements. Further, the implementation of allowlisting or blocklisting may be used to enforce execution of software to only software that has been authorized by the organization. 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 that 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 SP800-171 Reference: 3.4.9

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ASSET-3d	Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHITECTURE-1e)
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

Discussion:

Fully Implementing or Largely Implementing ASSET-3d, ASSET-3e, and ARCHITECTURE-3d would likely provide a similar capability 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. While users may have a business need for installing software that is not included in standard baselines, additional software may introduce additional 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.L1-3.5.1

CMMC Short Name: Identification

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

NIST SP800-171 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 would likely provide a similar capability to IA.L1-3.5.1. To meet CMMC IA requirements, organizations may need to tighten up current practices around identities.

With regards to identification, access to most systems will require a unique identifier; sharing is not generally allowed unless required for operational requirements. Also, ad-hoc management of users, devices, and processes needs to be more formal. Maintain accurate lists of what is allowed to access your systems. Without these lists, it is difficult if not impossible, to detect an unauthorized access. Organization may consider codifying these requirements in an IA policy to ensure users are aware that their actions are traceable to individual users and devices.

IA.L1-3.5.2

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 SP800-171 Reference: 3.5.2

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

Discussion:

Fully Implementing or Largely Implementing ACCESS-2a would likely provide the same capability as IA.L1-3.5.2. Like Identification, Authentication is a bit more formal in the CMMC framework and organizations should review if the potential artifacts that may be examined by an assessor are in place and maintained.

Organizations should consider documenting how systems are accessed, who is responsible for tracking credentials, and have a policy in place to revoke credentials when a device is decommissioned, or a user leaves the organization. In addition, documentation and policy around authentication may also include requirements around best practices like 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 SP800-171 Reference: 3.5.3

DoD 800-171 Assessment Methodology Point Value: 0

Related C2M2 Practices

ACCESS-1f	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)

Discussion:

Fully Implementing or Largely Implementing ACCESS-1f would likely provide a similar capability to IA.L2-3.5.3. Another way to look at this practice is to determine the single scenario when MFA is NOT required: local access (i.e., sitting at the keyboard of your laptop), logging into it with a non-privileged (not local admin) account, and not connecting to an organization’s network. This CMMC practice requires MFA in all other instances.

As a matter of best practice, organizations should consider MFA on all devices and accounts where it can possibly be enabled and enforced. There are some instances where implementing MFA will not be feasible, such as with legacy devices or OT devices that do not have the capability. In instances where MFA cannot be enabled, organizations may consider implementing compensating controls to meet the cybersecurity requirements of the organization. Multifactor authentication is not required for access to mobile devices such as smartphones or tablets – which are not considered to be 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 SP800-171 Reference: 3.5.4

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

While there is no analogous practice in C2M2, this is typically found in all commercial products. Ensure your policies require it and verify any in-house developed applications and devices use employ replay-resistant authentication mechanisms.

Replay-resistant authentication is important because it ensures that even if network traffic is intercepted by an attacker, they could not use the captured data to authenticate them at a later time. For example, the Kerberos authentication protocol operates on “tickets” that must be requested by a subject to access a resource. These 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 SP800-171 Reference: 3.5.5

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This CMMC practice does not have a direct relationship with C2M2. Organizations should consider how policies and procedures enable them to meet the assessment objectives of this CMMC practice.

Ensure your policies specify a period where identifiers are not reused and demonstrate how you implement it. Combine this with how identifiers are retired (i.e, when an employee leaves the organization). In most organizations, identifiers are never reused.

IA.L2-3.5.6

CMMC Short Name: Identifier Handling

Disable identifiers after a defined period of inactivity.

NIST SP800-171 Reference: 3.5.6

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ACCESS-1e	Identities are deprovisioned within organization-defined time thresholds when no longer required

Discussion:

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

Ensure that the threshold you choose is defined in your IA management policy and be prepared to demonstrate system settings that enforce that policy. In addition to using technology to disable unused accounts, a periodic review (organizationally defined) of accounts and verifying they were disabled by practice (on an employee's last day for instance) 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 SP800-171 Reference: 3.5.7

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

New ACCESS practice (proposed) - otherwise, there is only an intersection with ACCESS-2c	Password strength and reuse restrictions are defined and enforced

Discussion:

Fully Implementing or Largely Implementing ACCESS-2d would likely provide a similar capability to IA.L2-3.5.7. Ensure your password requirements are well defined and communicated in an IT User Policy along with your IA policy. Configure systems to require the same complexity definition and prevent incremental passwords, defined words, and sequential or repeating characters.

In general, longer is better and passphrases are recommended over passwords. 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 SP800-171 Reference: 3.5.8

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

New ACCESS practice (proposed) - otherwise, there is only an intersection with ACCESS-2c	Password strength and reuse restrictions are defined and enforced

Discussion:

Fully Implementing or Largely Implementing ACCESS-2d would likely provide a similar capability to IA.L2-3.5.8. Defining these requirements in documentation, such as an IA policy, would serve as a basis for those who are implementing controls to enforce reuse restrictions.

As with C2M2, document your reuse policy and ensure it Is communicated through the organization. Verify that your systems are configured to enforce the requirement. Generational reuse is related to your password change frequency and complexity. Collectively, the way you approach this needs to support the business and 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 SP800-171 Reference: 3.5.9

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This CMMC practice does not have a direct relationship with C2M2, but it is the default on many IT systems. Organizations should carefully consider if the default credentials for all IT and OT devices have been updated to organizational requirements.

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

IA.L2-3.5.10

CMMC Short Name: Cryptographically-Protected Passwords

Store and transmit only cryptographically-protected passwords.

NIST SP800-171 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 (ASSET-2d)

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-5d would likely provide a similar capability to IA.L2-3.5.10. Though 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 is likely the default behavior of most assets. While this may not be true for some OT assets, those assets would not be assessed against this CMMC practice. It is important to note that organizations are still required to have risk-based security policies, procedures, and practices for these assets.

IA.L2-3.5.11

CMMC Short Name: Obscure Feedback

Obscure feedback of authentication information.

NIST SP800-171 Reference: 3.5.11

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

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

Most assets display a generic character when a user is entering a password by default. Assets may not need additional configuration to meet this CMMC practice, but the 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 SP800-171 Reference: 3.6.1

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

RESPONSE-3d	Cybersecurity incident response plans that address all phases of the incident lifecycle are established and maintained
RESPONSE-5b	Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain

Discussion:

Fully Implementing or Largely Implementing RESPONSE-3d and RESPONSE-5b would likely provide a similar capability as the one required by IR.L2-3.6.1. This CMMC practice requires an organization have established an incident handling program that covers all phases of an incident. 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, are included in NIST Special Publication 800-61 Rev. 2 *Computer Security Incident Handling Guide*.

Establishing an incident handling capability should begin with the development of a policy and plan that guide the creation of the program and give authority to the program lead. These documents will provide the direction necessary to hire or assign individuals to the team and the justification for the purchase of necessary tools. Next, the team should draft procedures that outline the steps staff should take when responding to an incident. 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. The organization should also consider activities that should 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 SP800-171 Reference: 3.6.2

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

RESPONSE-2f	There is a repository where cybersecurity events and incidents are logged and tracked to closure
RESPONSE-2g	Cybersecurity stakeholders (for example, government, connected organizations, vendors, sector organizations, regulators, and internal entities) are identified and notified of events and incidents based on situational awareness reporting requirements (SITU

Discussion:

Fully Implementing or Largely Implementing RESPONSE-2f and RESPONSE-2g 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, the organization should establish a method for the incident lead to track and document information related to an incident. The organization may implement a tracking system that has workflows that ensure that necessary steps in the incident response process are performed and provides higher-level reporting to leadership. A system such as this might also assist the incident response team in notifying the necessary organizational officials of incidents and knowing when an incident requires that notification be provided to external authorities.

IR.L2-3.6.3

CMMC Short Name: Incident Response Testing

Test the organizational incident response capability.

NIST SP800-171 Reference: 3.6.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

RESPONSE-3f	Cybersecurity event and incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events
RESPONSE-4g	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-3f and RESPOSNE-4g would likely have a similar capability 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.

The organization should consider documenting a frequency by which incident response testing must be completed (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 would provide 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 SP800-171 Reference: 3.7.1

DoD 800-171 Assessment Methodology Point Value: 3

Related C2M2 Practices

ASSET-4d	Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement)

Discussion:

If an organization has Fully Implemented or Largely Implemented ASSET-4d, they may have a similar capability to MA.L2-3.7.1, but should review their 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 the guidelines set forth by manufacturers and to meet operational requirements. Examples of maintenance include activities like patching vulnerabilities, vendor recommended updates, and physical maintenance of assets. Change management practices may include the requirement to document the changes performed in a centralized repository. Changes performed by both the organization and third parties should documented. The 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 SP800-171 Reference: 3.7.2

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ASSET-4a	Changes to inventoried 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 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 may provide a similar capability to MA.L2-3.7.2, but the 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 a patch being applied that degrades system performance or running a tool that impacts network performance. Change management practices should define permitted tools, techniques, and mechanisms that may be used to conduct system maintenance. The organization should also consider which roles should be responsible for conducting system maintenance and 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 SP800-171 Reference: 3.7.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ASSET-1i	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 might provide a similar capability 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 any assets that are not under the control of the organization. This practice is specifically focused on CUI, but the organization should consider this activity for any other information that it deems to be sensitive. For CUI, it is recommended that organizations 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 SP800-171 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:

If an organization has Fully Implemented or Largely Implemented ARCHITECTURE-3g, they may have a similar capability to MA.L2-3.7.4, but should review their change management practices to ensure that they address the maintenance and CUI-specific requirements of CMMC.

Maintenance of assets may require that diagnostic or test applications be executed from removeable media by the organization or a third party. Removeable media should be tested to verify 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 SP800-171 Reference: 3.7.5

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ACCESS-1f	Stronger or multifactor credentials are required for access that poses higher risk to the function (such as privileged accounts, service accounts, shared accounts, and remote access)
ACCESS-1e	Identities are deprovisioned within organization-defined time thresholds when no longer required

Discussion:

If an organization has Fully Implemented or Largely Implemented ACCESS-1f and ACCESS-1e, they may have a similar capability to MA.L2-3.7.5, but should review their access control practices to ensure that they address the maintenance specific requirements of CMMC.

Some system maintenance may be conducted remotely by the organization or by a third party. For example, staff responsible for maintaining assets are located at a central facility and are also responsible for maintaining equipment at other satellite facilities. Some maintenance may need to be provided on-site, but other maintenance may be performed remotely. The organization should ensure that additional protections are implemented for performing these sensitive actions remotely. This may be achieved by a remote desktop session that requires multifactor authentication to initiate the connection and is automatically 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 SP800-171 Reference: 3.7.6

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

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

Discussion:

An organization that has Fully Implemented or Largely Implemented ACCESS-3i may have a similar capability to MA.L2-3.7.6, but should review access control procedures to ensure they meet the CMMC maintenance-specific requirements.

Sensitive areas of a facility, such as process control rooms, will likely have restricted physical access requirements to limit access to employees who need to access the area 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 cases, these employees have prior physical access authorization. Organizations should also consider procedures for supervising those who do not have authorization but are required to perform maintenance. For example, a vendor must be brought onsite to perform maintenance of process control devices. While this maintenance is being performed, they must be escorted by someone who verifies the actions they are taking to ensure they do not impact the overall process.

MEDIA PROTECTION

MP.L1-3.8.3

CMMC Short Name: Media Disposal

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

NIST SP800-171 Reference: 3.8.3

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ASSET-1i	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-1i may provide some of the capability of MP.L1-3.8.3, but organizations should review the FCI-specific requirements of this CMMC practice. Media must be properly sanitized or destroyed prior to disposal or reuse. In addition to shredding paper media, devices which store CUI can be physically destroyed or logically wiped or overwritten depending on the type of device. It is not limited to obvious storage devices such as disk drives and DVDs. USB drives, mobile phones and tablets, and printers can all store data and need to be properly handled until control is surrendered.

NIST SP 800-88 provides guidance on media sanitization. Many organizations incorrectly reference legacy instructions in DoD 5220.22 in their media disposal policies. Ensure you structure your disposal requirements around 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 SP800-171 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 determined (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 may provide a similar capability to MP.L2-3.8.1, but organizations should review the CUI-specific requirements of this practice. CMMC requires that you control physical access to CUI in addition to providing 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.

Storage in locked containers, electronic locks on doors (i.e. badging), access logs, etc. are all methods of tracking CUI access to physical media. Since your organization controls many types of protected and otherwise controlled information, include CUI as a category of information you protect in your 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 SP800-171 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 is 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 would likely provide a similar capability to MP.L2-3.8.2, but organizations should review the CUI-specific requirements of this CMMC practice.

This practice is really an extension of MP.L2-3.8.1 and requires that in addition to protecting the media you have policies and procedures in place to determine who has access to the physical CUI, track who does access 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 SP800-171 Reference: 3.8.4

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This CMMC practice does not have a direction relationship with C2M2 due to the CUI-specific nature of the requirements. CUI requires special markings which differ depending on the category of CUI. The U.S. National Archives and Records Administration (NARA) is the executive agent for CUI and has a marking handbook available at on the NARA CUI program page along with training material for how to correctly mark CUI.

Guidance covers physical and electronic marking; include this material in your CUI handling procedures and user training. DoD also provides additional CUI information and training at https://www.dodcui.mil/ including 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 SP800-171 Reference: 3.8.5

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This CMMC practice does not have a direction relationship with C2M2 due to the CUI-specific nature of the requirements. Related to your other media protection policies, in addition to controlling access to CUI, this practice adds accountability during transport outside of controlled areas. So, in addition to maintaining a check-in/check-out system, you need a mechanism to assign responsibility and accountability for the media when it is no longer within the physical confines of your controlled area.

NARA provides guidance and how to use tamper-evident packaging and label 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 SP800-171 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 (ASSET-2d)

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-5d would likely provide simiar capabilities to MP.L2-3.8.6, but organizations should review the CUI-specific requirements of this CMMC practice. Cryptographic controls are already in place for your C2M2 practice and its preferable to use them over alternative physical protections. CMMC imposes an additional requirement that encryption modules be FIPS 140-2 validated. You can lookup FIPS validated modules on the NIST CMVP website. Currently, FIPS 140-3 is being phased in; look for updates to CMMC assessment guides as NIST updates SP 800 series documents.

NIST SP 800-111 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 SP800-171 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 would likely provide the same capability as MP.L2-3.8.7. At a minimum, communicate your policy to all users and document it in your acceptable use policy, IT User Policy, and/or media control policy. Because of the risk of data exfiltration and loss and malware introduction, its best to implement technology 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 for use with other devices.

If business needs dictate the use of portable storage devices, it is suggested that only devices issues by the organization be used. This can be enforced through the same configurations that restrict the device. If transporting CUI on portable storage devices, consider a solution specifically made for that. The market offers several solutions that enforce FIPS validated encryption, restricts use to only the authorized devices and monitors 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 SP800-171 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 of the capability of MP.L2-3.8.8, but organization should review the requirements of this CMMC practice to determine if additional administrative or technical controls may be 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, your policy should prohibit these unknown devices but preferably you have technology in place to prevent the use of these 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 SP800-171 Reference: 3.8.9

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

RESPONSE-4h	Data backups are protected with at least the same controls as source data
ARCHITECTURE-5d	Cryptographic controls are implemented for data at rest and data in transit for selected data categories (ASSET-2d)

Discussion:

Fully Implementing or Largely Implementing REPONSE-4h and ARCHITECTURE-5d would likely provide a similar capability to MP.L2-3.8.9, but organizations should consider the CUI-specific requirements of this CMMC practice. Backup storage facilities should provide at least the same level of protection as the facility where the data is hosted. This can be by the same physical and logical controls employed at the host site. In order to be truly effective, a backup should be held in an alternate site, and this is 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. It should be noted that alternate physical protections would only apply to the transport of a physical storage device. When evaluating cloud backup options, ensure the backup is encrypted in transit using a FIPS 140-2 validated module. While virtually every backup option supports encryption, 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 SP800-171 Reference: 3.9.1

DoD 800-171 Assessment Methodology Point Value: 3

Related C2M2 Practices

WORKFORCE-3a	Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner
WORKFORCE-3c	Personnel vetting is performed periodically for positions that have access to the assets required for delivery of the function
WORKFORCE-3f	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-3a, WORKFORCE-3c, and, WORKFORCE-3f would likely provide a similar capability to PS.L2-3.9.1, but the CUI-specific requirements of this practice should be considered. The organization may need to modify existing vetting procedures to ensure that they meet this requirement.

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 SP800-171 Reference: 3.9.2

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

WORKFORCE-3b	Personnel separation procedures address cybersecurity, at least in an ad hoc manner
WORKFORCE-3d	Personnel transfer procedures address cybersecurity
ACCESS-2b	Logical access is revoked when no longer needed, at least in an ad hoc manner

Discussion:

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

An organization is preparing to gain work that would require them to obtain CMMC certification and the security team is working with the enterprise IT team on policies and procedures around employee transfer and termination. The teams develop a process for each of these situations that would get triggered by a notification from the HR team that an employee action has occurred. Following that notification, if an employee is being terminated, access to the organization’s network, systems, and applications is revoked. The process also includes steps where the organization ensures that all equipment is returned, physical access devices (e.g., keys, badges) are returned, and an exit interview is conducted.

PHYSICAL PROTECTION

PE.L1-3.10.1

CMMC Short Name: Limit Physical Access

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

NIST SP800-171 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 determined (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 would likely provide the same capabilities as PE.L1-3.10.1. Limiting physical access to organizational assets is important to ensure the organization can meet security and safety requirements.

Organizations should implement physical access controls that reduce the risk of an incident stemming from unauthorized access. This risk may vary based upon the assets within a physical space and 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 would likely present a greater risk than a storage facility. Organizations should consider which individuals should have access to systems, equipment, and operating environments, and only provide access to individuals who need access to these assets based on their job responsibilities.

PE.L1-3.10.3

CMMC Short Name: Escort Visitors

Escort visitors and monitor visitor activity.

NIST SP800-171 Reference: 3.10.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ACCESS-3g	Physical access that poses higher risk to the function receives additional scrutiny and monitoring

Discussion:

Fully Implementing or Largely Implementing ACCESS-3g would likely provide the same capability as PE.L1-3.10.3.

Organizations should implement controls to restrict and monitor physical access to facilities by unauthorized individuals. There may be exceptions where portions of a facility may be open to the public, for example a desk where a bill may be paid by a customer. The organization should have policies and procedures in place for situations where a visitor needs to access restricted areas of a facility (e.g., a safety inspection). Visitors should be always escorted when in restricted areas for safety and security. The organization should also implement a process to have visitors sign in and out of a facility and be assigned a visitor badge.

PE.L1-3.10.4

CMMC Short Name: Physical Access Logs

Maintain audit logs of physical access.

NIST SP800-171 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 would likely provide the same capability as PE.L1-3.10.4.

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

PE.L1-3.10.5

CMMC Short Name: Manage Physical Access

Control and manage physical access devices.

NIST SP800-171 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 is revoked when no longer needed, at least in an ad hoc manner
ACCESS-3d	Physical access requirements are determined (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)
ACCESS-3h	Physical access privileges are reviewed and updated

Discussion:

Fully Implementing or Largely Implementing ACCESS-3a, ACCESS-3b, ACCESS-3d, and ACCESS-3h would likely provide the same capability as PE.L1-3.10.5. Similar to assigning logical access identities, physical access devices should be assigned to authorized employees to control physical access.

It is important that the organization has a record of who has been assigned assets like keys, badges, or combinations to locks. This may be achieved by keeping a log and having employees sign when receiving one of these assets. Employees should be held accountable for protecting these assets and only using them for authorized purposes. The organization should also consider implementing revocation of these assets into procedures for employee transfer or termination. It may also be necessary to consider processes for changing locks or combinations in situations where an asset is not in control of an authorized individual.

PE.L2-3.10.2

CMMC Short Name: Monitor Facility

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

NIST SP800-171 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-3i	Physical access is monitored to identify potential cybersecurity events

Discussion:

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

This CMMC practice requires implementation of controls to protect and monitor the physical facility, as well as support infrastructure. Access controls may be implemented in a variety of methods, such as fences, doors with locks or badge readers, or guard checkpoints. It is equally important that physical access is monitored, which may be achieved through methods, such as video cameras and review of access logs. These controls for protecting and monitoring the physical space should be reviewed to determine if they are providing 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 SP800-171 Reference: 3.10.6

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ASSET-2c	The information asset inventory includes attributes that support cybersecurity activities (for example, backup locations and frequencies, storage locations, cybersecurity requirements)
ACCESS-3d	Physical access requirements are determined (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access)
ARCHITECTURE-1e	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 (ASSET-2d)

Discussion:

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

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

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 SP800-171 Reference: 3.11.1

DoD 800-171 Assessment Methodology Point Value: 3

Related C2M2 Practices

RISK-2c	Cyber risk identification leverages multiple risk identification techniques and information sources
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

Discussion:

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

The CMMC practice specifically calls out risks related to CUI but that should just be one category of risk an organization’s overall Risk Assessment. And while C2M2 specifically mentions cyber risks, CMMC casts a wider net and includes things like business processes, natural disasters, and third parties.

Organizations should consider how Risk Assessment activities relate to other governing policies, such as a Disaster Recovery Plan or Business Continuity Plan. While the RA should be reviewed and updated as needed at least annually, it should also be reviewed following any significant change to the organizations 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 SP800-171 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 would likely provide the same capability as RA.L2-3.11.2. In both frameworks organizations are expected to perform vulnerability scanning when there are significant system changes, new vulnerabilities are identified and on an organizationally defined frequency. Somewhere in IT maintenance or risk management polies, organizations should consider documenting the scan interval and be prepared to show evidence (i.e. the scan reports) that these were performed.

Monthly scanning is generally regarded as a reasonable interval and is effective. When significant, zero-day threats are announced is also a good time to run out of cycle scans. CMMC requires scanning of systems and applications so ensure your approach covers all your devices. The best approaches use a combination of agent-based scans (where an agent reside on the endpoint and provides “continuous” scanning) and enterprise scans where a scanner runs across your environment to check devices which do not host an agent.

If using cloud services, the CSP will typically block independent scans of their environment, but they should be performing them as part of their SLAs and/or contracts. With the continued use of hybrid and remote work environments, traditional scanning will not always capture devices not connected to the organizational infrastructure. Ensure your approach does not exclude these remote devices. And while 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 SP800-171 Reference: 3.11.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

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-1k	Identified vulnerabilities that pose ongoing risk to the function are referred to the risk management program for response
RISK-4a	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risk categories and cyber risks, at least in an ad hoc manner

Discussion:

Fully Implementing or Largely Implementing THREAT-1d, THREAT-1g, THREAT-2k, and RISK-4a would 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 likely to be acceptable in an assessment. Your remediation plan should be tightly woven in with the overall Configuration Management Plan, your Risk Assessment, and your maintenance strategy.

Since not all vulnerabilities have equal impact, your ability to patch or mitigate them is largely dependent on the severity, the potential impact to you if exploited, and the business impact to deploy the fix. Guidelines to help in your decision process should be part of your Risk Assessment.

Any vulnerability not fixed should be tracked in the organization’s risk register and POAM including those where a mitigation has been implemented, but an additional fix is necessary 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 SP800-171 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 would likely provide some of the capability of CA.L2-3.12.1, but the additional assessment frequency requirement of the CMMC practice should be considered.

Organizations should evaluate if security controls that have been 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 will give assurance that security controls and countermeasures are sufficient to reduce potential risks to organizational risk tolerances. Organizations may also consider documenting a standard that should 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 SP800-171 Reference: 3.12.2

DoD 800-171 Assessment Methodology Point Value: 3

Related C2M2 Practices

RISK-4a	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risk categories and 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
THREAT-1k	Identified vulnerabilities that pose ongoing risk to the function are referred to the risk management program for response

Discussion:

Fully Implementing or Largely Implementing RISK-4a, RISK-4b, and THREAT-1k would likely provide a similar capability as 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. This decision may be based on constraints, such as funding, resource availability, or scheduling. To meet this CMMC practice, organizations should ensure that documentation that is developed to address planned remediations 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 POAM template on the NIST SP 800-171 Rev. 2 webpage.

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 SP800-171 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 would 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 performing these evaluations on an ongoing basis. The organization should consider developing a defined process for evaluating and analyzing control effectiveness at a frequency that will support organizational risk management decisions. In addition, the organization should consider methods to communicate these 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 SP800-171 Reference: 3.12.4

DoD 800-171 Assessment Methodology Point Value: 0

Related C2M2 Practices

ARCHITECTURE-1b	A strategy for cybersecurity architecture is established and maintained to support 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-1e	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-1e would likely provide a similar capability to CA.L2-3.12.4, but organizations should consider the CMMC-specific requirements of this practice.

System security plans (SSPs) are one of the primary documents that organizations are required to develop and maintain when operating a covered contractor information system and would likely be requested during 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 webpage.

SYSTEMS AND COMMUNICATIONS PROTECTION

SC.L1-3.13.1

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 SP800-171 Reference: 3.13.1

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2b	Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements (ASSET-1a, ASSET-2a)
ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])
ARCHITECTURE-2f	Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking)
ARCHITECTURE-2j	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2b, ARCHITECTURE-2e, ARCHITECTURE-2f, and ARCHITECTURE-2j would likely provide a similar capability to SC.L1-3.13.1. The organization should consider the location of network protection devices to ensure they are implementing adequate monitoring and control of network traffic at internet and external network boundaries.

Network protection devices like firewalls are vital to controlling network traffic and protecting the network from unwanted or malicious traffic. Other devices like gateways and routers manage the flow of traffic and can be used to implement subnets. It is important for organizations to first evaluate and document system boundaries to determine if current network protection devices are providing adequate security for sensitive information.

Additional controls may need implemented 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.L1-3.13.5

CMMC Short Name: Public-Access System Separation

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

NIST SP800-171 Reference: 3.13.5

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2a	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

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2a may provide similar capability as SC.L1-3.13.5, but the organization should give additional consideration to assets that are publicly accessible. It is important to separate these assets from the internal network as 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 these assets, the organization should then review if sufficient segmentation is in place to separate these assets from the internal network. It is common practice to place all publicly accessible assets into a separate demilitarized zone (DMZ) segment of the network that is outside of the internal network. This architectural tactic helps mitigate the risk of an attacker compromising a publicly accessible system and moving laterally. The organization may consider testing, such as 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 SP800-171 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-1e	The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets
ARCHITECTURE-1f	Cybersecurity controls are selected and implemented to meet cybersecurity requirements
ARCHITECTURE-1h	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 (ASSET-1d) is developed using secure software development practices
ARCHITECTURE-4c	Secure software configurations are required as part of the software deployment process
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 e

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-1c, ARCHITECTURE-1e, ARCHITECTURE-1f, ARCHITECTURE-1h, ARCHITECTURE-4a, ARCHITECTURE-4c, ARCHITECTURE-4d, ARCHITECTURE-4f, and ARCHITECTURE-4h may provide some similar capabilities to SC.L2-3.12.2, but organizations should consider the necessary system engineering-specific requirements of this CMMC practice. Implementation of these C2M2 practices would enable organizations to consistently employ system and network protections that meet protection requirements and produce secure software. 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 should be reviewed for applicability to system development activities.

The cybersecurity program should consider how cybersecurity requirements apply to different types of assets and document these requirements in a cybersecurity architecture. The establishment of a cybersecurity architecture provides a reference for those implementing security controls to ensure that they meet defined cybersecurity requirements for the organization's assets. Similarly, requirements for developing secure software should be established and used 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 SP800-171 Reference: 3.13.3

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-2b	Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements (ASSET-1a, ASSET-2a)
ARCHITECTURE-2g	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 ARCHITECTURE-2b, ARCHITECTURE-2g, and ARCHITECTURE-3c would likely provide a similar capability to SC.L2-3.13.3. The core of this CMMC practice is Is the principle of least privilege and requires additional logical or physical separation to enforce this principle.

Organizations should identify the system management activities that are necessary for operations and determine the methods that are used to access these sensitive functions. It might be necessary to document which activities should only be completed from specific systems or with different credentials in policies. This CMMC practice requires additional separation of the management of systems through logical of physical means to ensure that only a limited number of users have access to these sensitive functions. For example, a network security engineer needs to conduct maintenance of a firewall and implement new rules based on threat intelligence. This may be achieved by logging into a separate administrative account on a virtual machine that is 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 SP800-171 Reference: 3.13.4

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-3e	Secure configurations are implemented as part of the asset deployment process where feasible

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-3e may provide similar functionality to SC.L3-3.13.4. The organization should continually review the configuration of assets to ensure that mitigations are in place for newly discovered vulnerabilities.

This CMMC practice could likely leverage other activities like 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 that would prevent unauthorized or unintended information transfer. System configurations and configuration baselines should be continuously reviewed and updated to mitigate newly discovered vulnerabilities that could allow the discloser 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 SP800-171 Reference: 3.13.6

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])

Discussion:

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

Firewalls are a common way to restrict network traffic, but they are only as effective as the rules that they use to filter traffic. This CMMC practice requires that firewalls and other network protection devices be configured to deny all network traffic and only allow traffic by exception. When implementing firewall rules, the organization must carefully consider 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 SP800-171 Reference: 3.13.7

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2e may provide the same capability as SC.L2-3.13.7, but configurations should be reviewed to ensure the meet the specific requirements of this CMMC practice.

Split tunneling allows a system to establish a connection between two networks, such as a system simultaneously connecting to the organization's trusted VPN and an external network like the Internet. Implementation of controls to prevent split tunneling will help reduce the potential of an attacker exfiltrating information or using a trusted system as an initial point of entry into the organization's network. Preventing users from using split tunneling should be considered during the creation of configuration baselines and be a consideration of the 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 SP800-171 Reference: 3.13.8

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 (ASSET-2d)

Discussion:

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

Organizations must ensure that adequate controls are implemented to protect sensitive data, such as CUI. Data in transit may be protected by cryptographic mechanisms like a TLS connection between two systems. If cryptography is selected as the method to meet this CMMC practice, it is required that encryption is implemented using FIPS-validated cryptography. The cryptographic module used to implement the algorithm must be validated under FIPS 140. Organizations may also choose to implement physical protections instead of cryptography in situations where encryption would not be feasible or would be impractical. Organizations may refer to the US government requirements for protected distribution systems (PDS) that protect unencrypted national security information. A PDS may 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 SP800-171 Reference: 3.13.9

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ASSET-3c	The design of configuration baselines includes cybersecurity objectives
ARCHITECTURE-2d	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 dev
ARCHITECTURE-3a	Cybersecurity controls are implemented for assets important to the delivery of the function, at least in an ad hoc manner

Discussion:

Fully Implementing or Largely Implementing ASSET-3c, ARCHITECTURE-2d, and ARCHITECTURE-3a may provide a similar capability to SC.L2-3.13.9, but configurations should be reviewed to ensure the meet the specific requirements of this CMMC practice.

An unattended workstation may be leveraged by an insider threat 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 and define them in a document, such as a policy. Configuration baselines should adhere to this requirement and assets like applications should also 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 SP800-171 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 would likely provide the same capability as SC.L2-3.13.13.

Cryptographic keys may 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 only effective if they are properly managed. The organization should have clearly defined policies and procedures for establishing and managing cryptographic keys. This 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 SP800-171 Reference: 3.13.11

DoD 800-171 Assessment Methodology Point Value: 0

Related C2M2 Practices

ARCHITECTURE-5d	Cryptographic controls are implemented for data at rest and data in transit for selected data categories (ASSET-2d)

Discussion:

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

It is important to note that any cryptography used to protect the confidentiality of CUI must be validated by the NIST Cryptographic Module Validation Program (CMVP). More details on the CMVP and a listing of validated modules can be found on the CMVP website. The focus of this practice is the use of validated cryptography, while SC.L2-3.13.8 requires encryption for CUI in transit and SC.L2-3.13.16 requires encryption for CUI that is at rest. It is noted in the CMMC L2 Assessment Guide that "…FIPS-validated cryptography is required to meet CMMC practices 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 SP800-171 Reference: 3.13.12

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

Discussion:

This CMMC practice does not have a related C2M2 practice.

Organizations may implement collaborative computing devices, such as video conferencing systems, in conference rooms or other shared spaces to enable meetings with remote participants. If a conference room is being used to discuss sensitive information, an attacker could potentially activate these devices to exfiltrate sensitive information. It is important to identify these devices and ensure that they are configured to prohibit remote activation to mitigate against this attack. Similarly, devices should only be used 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, the organizations 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 SP800-171 Reference: 3.13.13

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-3e	Secure configurations are implemented as part of the asset deployment process where feasible
ARCHITECTURE-3j	Controls are implemented to prevent the execution of unauthorized code

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-3e and ARCHITECTURE-3j would likely provide a similar capability to SC.L2-3.13.13. In addition to technical controls, the organization would need to consider policies that document usage restrictions.

Mobile code is defined 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." [800-171r2] Examples of mobile code include JavaScript, ActiveX, and VBScript. Since mobile code may be used by an attacker to execute malicious code, organizations should consider what types of mobile code are necessary to meet business requirements. The 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. Controls should be implemented that enable the organization 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 SP800-171 Reference: 3.13.14

DoD 800-171 Assessment Methodology Point Value: 1

Related C2M2 Practices

ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])
ARCHITECTURE-2j	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2e and ARCHITECTURE-2j may provide a similar capability as SC.L2-3.13.14, but organizations should review the specific requirements of this CMMC practice.

Voice over Internet Protocol (VoIP) technology may 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 could be leveraged to ensure that VoIP traffic is controlled and monitored like other network traffic. Technical controls should be considered to prevent this disruption or interception of VoIP traffic and to enforce the use of approved VoIP technologies. Organizations should also consider documenting which VoIP technologies are approved for use by users, along with acceptable use of these technologies.

SC.L2-3.13.15

CMMC Short Name: Communications Authenticity

Protect the authenticity of communications sessions.

NIST SP800-171 Reference: 3.13.15

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])
ARCHITECTURE-2j	Network connections are protected commensurate with risk to the organization (for example, secure connections for remote administration)

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2e and ARCHITECTURE-2j would likely provide a similar capability 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 mitigates against 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 could 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 SP800-171 Reference: 3.13.16

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 (ASSET-2d)

Discussion:

capability as SC.L2-3.13.16, but the organization should review the CUI-specific requirements of this CMMC practice.

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 the 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 in situations where encryption is not feasible or impractical. For example, a database that contains CUI can only be accessed by workstations that are located in a physically controlled room.

SYSTEM AND INFORMATION INTEGRITY

SI.L1-3.14.1

CMMC Short Name: Flaw Remediation

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

NIST SP800-171 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 similar capabilities to SI.L1-3.14.1, but organizations should consider the specific time frame requirements of this CMMC practice. While C2M2 allows for an ad-hoc process for remediation, CMMC requires more structure. You will need to show that you have established time standards to identify, report, and correct flaws. Additionally, be prepared to show proof that your procedures have allowed you to meet those timelines. If unable to meet the timelines (i.e., operational constraints prohibit restating a system), document the risk (POA&M) and set a target for fixing it.

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

While 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.L1-3.14.2

CMMC Short Name: Malicious Code Protection

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

NIST SP800-171 Reference: 3.14.2

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

ARCHITECTURE-2e	Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, whitelisting, intrusion detection and prevention systems [IDPS])
ARCHITECTURE-2f	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-3j	Controls are implemented to prevent the execution of unauthorized code

Discussion:

Fully Implementing or Largely Implementing ARCHITECTURE-2e, ARCHITECTURE-2f, ARCHITECTURE-3f, and ARCHITECTURE-3j would likely provide a similar capability to SI.L1-3.14.2. In the context of CMMC, this will tie into configuration management policies as locations requiring protection need to be identified. In addition to endpoint protection, prioritizing cloud services may be considered as filtering network traffic before it enters the network boundary may help achieve cybersecurity objectives.

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

SI.L1-3.14.4

CMMC Short Name: Update Malicious Code Protection

Update malicious code protection mechanisms when new releases are available.

NIST SP800-171 Reference: 3.14.4

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

Discussion:

While there is no analogous C2M2 practice, it is likely that malicious code protection mechanisms meet this requirement by default. Ensure that whatever anti-malware solutions are deployed are updated regularly. The update frequency should be defined and the tools configured to ensure 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.L1-3.14.5

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 SP800-171 Reference: 3.14.5

DoD 800-171 Assessment Methodology Point Value: 3

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 would like provide some of the same capability as SI.L1-3.14.5, but organization should review security tool configurations to ensure they meet the requirements of this CMMC practice. Generally, deployed anti-malware tools will scan on access or in transit by default. Real time scans can occur at multiple times as well; while browsing, in the cloud before it enters the organization’s email system, and anytime a file is accessed.

CMMC also requires that periodic full scans of systems are executed. While there is no defined time for these scans, STIGs for some of the more common AV software require full scans to occur at least weekly and some systems may require a validation check before you can use that device to connect. Regardless of the method employed, ensure its 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 SP800-171 Reference: 3.14.3

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

SITUATION-2c	Monitoring and analysis requirements are established and maintained for the function and address timely review of event data
SITUATION-2e	Alarms and alerts are configured and maintained to support the identification of cybersecurity events
THREAT-2f	Identified threats are analyzed and prioritized and are addressed accordingly
RISK-4a	Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risk categories and cyber risks, at least in an ad hoc manner
THREAT-1l	Vulnerability monitoring activities include review and confirmation of actions taken in response to cybersecurity vulnerabilities where appropriate

Discussion:

Fully Implementing or Largely Implementing SITUATION-2c, SITUATION-2e, THREAT-2f, RISK-4a, and THREAT-1l would likely provide a similar 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 just some of the sources to monitor.

Once identified, ensure a documented process to notify affected stakeholders and take corrective action as needed is in place. Ensure that external service providers 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 SP800-171 Reference: 3.14.6

DoD 800-171 Assessment Methodology Point Value: 5

Related C2M2 Practices

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 SITUATION-2c, SITUATION-2d, and SITUATION-2e will likely provide the same capability as SI.L2-3.14.6. Ensure that audit and retention practices are in line with the requirements of this CMMC practice. Automated tools make for a much easier and effective practice.

SI.L2-3.14.7

CMMC Short Name: Identify Unauthorized Use

Identify unauthorized use of organizational systems.

NIST SP800-171 Reference: 3.14.7

DoD 800-171 Assessment Methodology Point Value: 3

Related C2M2 Practices

WORKFORCE-4a	Cybersecurity awareness activities occur, at least in an ad hoc manner
ACCESS-2i	Anomalous logical access attempts are monitored as indicators of cybersecurity events
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-2h	Continuous monitoring is performed across IT and OT environments to identify anomalous activity

Discussion:

Fully Implementing or Largely Implementing WORKFORCE-4a, ACCESS-2i, SITUATION-2d, and SITUATION-2h will likely provide a similar capability 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 stronger implementation.

APPENDIX B: APPYING CMMC TO C2M2

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

THIS SECTION WILL BE UPDATED FOR C2M2 V2.1

Asset, Change, and Configuration Management (ASSET)

C2M2 Practice		**CMMC Practice**	
ASSET-4e	Changes to assets are tested for cybersecurity impact prior to being deployed	CM.L2-3.4.4	Analyze the security impact of changes prior to implementation.

Threat and Vulnerability Management (THREAT)

C2M2 Practice		**CMMC Practice**	
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 Practice**	
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.L1-3.5.1	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.L1-3.5.2	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.L1-3.10.4	Maintain audit logs of physical access.

Cybersecurity Architecture (ARCHITECTURE)

C2M2 Practice		**CMMC Practice**	
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	Cryptographic controls are implemented for data at rest and data in transit for selected data categories (ASSET-2d)	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 2.0.* Retrieved MMM DD, 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, Version 2.1.* Retrieved MMM DD, 2022, from: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[CMMC L2 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://www.acq.osd.mil/cmmc/documentation.html

[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://www.acq.osd.mil/cmmc/documentation.html

[CMMC L2 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://www.acq.osd.mil/cmmc/documentation.html

[NIST SP800-171]
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