Maritime Bulk Liquids Transfer Cybersecurity Framework Profile

Table of Contents

List of Figures

List of Tables

Executive Summary

White House Executive Order (EO) 13636 tasked the Director of the National Institute of Standards and Technology (NIST) to "lead the development of a framework to reduce cybersecurity risks to critical infrastructure (the ''Cybersecurity Framework'')." The "Cybersecurity Framework" was published in February 2014, and the important work of integrating the framework into organizational operations is well underway in many industries. One of the primary ways industries are integrating the Cybersecurity Framework is by creating industry-focused Framework Profiles ("Profiles") as described in the Cybersecurity Framework.

The United States Coast Guard (USCG) is working with industry to develop voluntary Cybersecurity Framework Profiles (CFP) to mitigate risks in their joint mission areas. The USCG selected the Maritime Bulk Liquids Transfer (MBLT) mission area to complete the first Profile. The MBLT CFP identifies and prioritizes the minimum subset of Cybersecurity Framework Subcategories required to conduct BLT operations in a more secure manner, while giving organizations the flexibility to address Subcategories in whatever way makes the most sense for their unique risk posture.

Background

Although MBLT operations have not always relied on combined IT and OT processes, they are increasingly evolving towards a combined reliance. This introduces new cybersecurity risks that MBLT operators are working to manage. Appropriate security controls must be in place to support the proper operation of organizational processes such as human resources, training, and business communication. Likewise, OT security controls for storage, security, transfer, equipment, pressure monitoring, vapor monitoring, emergency response, and spill mitigation readiness must all be in place, inspected, and ready for operational use. Cybersecurity risks to MBLT can only be appropriately managed through an integrated assessment, mitigation, and recovery strategy for both IT and OT systems. MBLT is part of a complex and sophisticated supply chain in the oil and natural gas (ONG) industry with interdependencies between various types of organizations and systems. The MBLT mission area covers a blend of enterprise IT and OT. Both technologies must provide the proper data inputs so Mission Objectives and mission needs are satisfied in a safe and secure manner. Interdependencies between IT and OT can create multiple risks for the enterprise that must be managed. Cybersecurity risks are part of the enterprise risk environment, and some of those risks arise from IT systems used to support OT systems.

The Profile

This MBLT CFP serves to assist in cybersecurity risk assessments for those entities involved in MBLT operations as overseen by the USCG. It is intended to act as non-mandatory guidance to organizations conducting MBLT operations within facilities and vessels under the regulatory control of the USCG under the Code of Federal Regulations (CFR) 33 CFR 154-156. This MBLT CFP serves to collect recommended cybersecurity safeguards and describes the desired minimum state of cybersecurity for those organizations in the MBLT context.

The USCG consulted NIST regarding its work on the Cybersecurity Framework, and as a result of those discussions determined that an industry-focused CFP should be created for the various missions. NIST personnel who oversaw the development of the Cybersecurity Framework along with personnel from its National Cybersecurity Center of Excellence (NCCoE) have worked with industry and the USCG to develop Cybersecurity Framework Profiles that can be used by industry to assess their cybersecurity posture and readiness regarding several USCG mission areas.

During the development of the MBLT CFP, the team engaged Maritime and BLT operations subject matter experts. Their collective expertise was used in identifying the Mission Objectives and identifying the priority Cybersecurity Framework Categories and Subcategories for each Mission Objective.

Benefits

Creating an industry-focused Cybersecurity Framework Profile for MBLT has the following benefits:

- compliance reporting becomes a byproduct of running the organization's security operation
- adding new security requirements is more straightforward
- adding or changing operational methodology is less intrusive to ongoing operations
- minimizes future work by individual organizations
- decreases the chance that organizations accidentally omit a requirement
- facilitates understanding of the BLT environment to allow for consistent analysis of cybersecurity-risk
- aligns industry and USCG cybersecurity priorities

This Profile also enables strategic communications between:

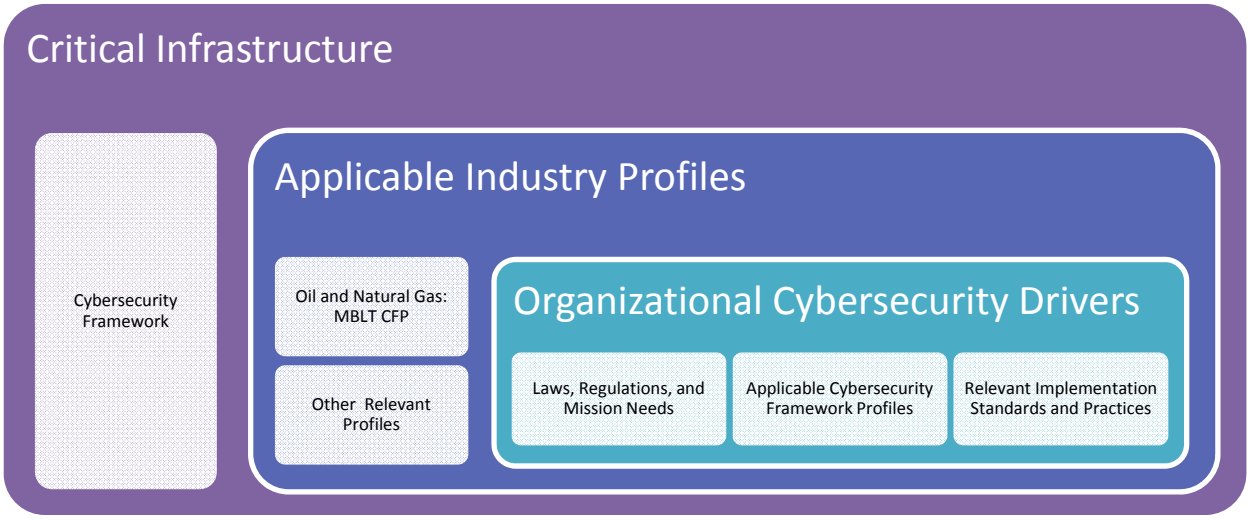
- risk executives and operational technology integration of cybersecurity capabilities
- personnel involved in cybersecurity governance processes and operational technology oversight
- enterprises who are just becoming aware of cybersecurity recommended practices with subject matter expertise and the collective wisdom of industry experts

1. Introduction

1.1. Purpose

This Maritime Bulk Liquids Transfer (MBLT) Cybersecurity Framework Profile (CFP) is an industry-specific instantiation of the Cybersecurity Framework Profile concept for a subsector of the oil and natural gas industry (ONG).[1] It is intended to act as non-mandatory guidance to organizations conducting MBLT operations within facilities and vessels under the regulatory control of the USCG under the Code of Federal Regulations (CFR) 33 CFR 154-156. This MBLT CFP collects recommended cybersecurity safeguards and describes the desired minimum state of cybersecurity for those organizations in the MBLT context in support of those safety-oriented regulations. This guidance serves to assist in cybersecurity risk assessments for those entities involved in MBLT operations as overseen by the USCG. The prioritized cybersecurity activities in the MBLT Profile act as a starting point for enterprises to review and adapt their risk management processes due to increased awareness of cybersecurity threats in the OT environment. Figure 1-1 shows the relationship between the Cybersecurity Framework, Cybersecurity Framework Profiles (generally), and an organization's cybersecurity drivers.

Figure 1-1. Relationship Between Cybersecurity Framework and an Organization



1.2. Audience and How to Use this Document

The MBLT CFP is intended for use by executives, risk managers, cybersecurity professionals, vessel and facility operators, and others with a role in cybersecurity risk management for MBLT operations. This document should be used by those involved in overseeing, developing, implementing and managing the cybersecurity components of MBLT operations. Executive-level personnel should utilize the Executive Summary, Section 2, and Section 6, to gain an understanding of the purpose and scope of this MBLT CFP.

[1] As described in Section 1.1 of the Cybersecurity Framework, "A Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state)."

Managers should utilize all main chapters of the MBLT CFP. Implementers should use the entire document including all appendices to understand the need for the MBLT CFP and its specific contents.

1.3. Document Structure

The remainder of Section 1 provides an overview of Cybersecurity Framework Profiles and a description of MBLT CFP.

Section 2 provides background information on Critical Infrastructure, the cybersecurity risk in the MBLT enterprise, Information Technology (IT) and Operational Technology (OT), and the regulatory context.

Section 3 discusses the Cybersecurity Framework and its components, including background about how Profiles emerge from it.

Section 4 describes the approach used to create this Profile, activities to date, and the foundations for the Profile.

Section 5 gives a roadmap for organizations that plan to use the MBLT CFP, and provides a process for organizations to incorporate this Profile into cybersecurity risk management processes within their enterprise.

Section 6 identifies MBLT Mission Objectives and provides summary mappings to Cybersecurity Framework Functions, Categories, and Subcategories.

Appendix A provides detailed Subcategory specifications for each Mission Objective. Appendix B provides a section by section review of 33 CFR 154-156. Appendix C provides further resources regarding Cybersecurity Framework Profiles and assessment processes for other industries.

1.4. Overview of the MBLT CFP

The MBLT CFP uses the Cybersecurity Framework's five Functions that are defined in the Framework Core:

- Identify
- Protect
- Detect
- Respond
- Recover

Each of these Functions is broken into Categories and Subcategories that describe expected outcomes of cybersecurity activities. The Framework Core is described in Section 3.1 of the Cybersecurity Framework[2]. The development of a Profile, regardless of its intended user community, is a multi-step process. Figure 1-2 lists the Categories included in the Framework Core by the five Functions.

[2] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (last visited July, 1, 2016).

Figure 1-2. Framework Core: Functions and Categories

Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Implementing industry-specific Cybersecurity Framework Profiles in a way that is relevant to industry members depends on defining Mission Objectives that are meaningful in the context of industry activities. In order to align the Cybersecurity Framework with the mission needs of MBLT operations, the USCG worked with industry to define the key Mission Objectives that shape cybersecurity activities. These Mission Objectives provide the necessary context for identifying and managing cybersecurity risk. Cybersecurity practices for MBLT rely on the eight Mission Objectives:

1. Maintain Personnel Safety
2. Maintain Environmental Safety
3. Maintain Operational Security
4. Maintain Preparedness
5. Maintain Quality of Product
6. Meet HR Requirements
7. Pass Required Audits/Inspections
8. Obtain Timely Vessel Clearance

The Missions Objectives are defined in Section 6.1. In order to help organizations prioritize and allocate resources most effectively, the Subcategories have been assigned priority levels that are described in Section 6.1. Appendix A provides the full detailed MBLT CFP.

2. Background

2.1. Cybersecurity and the Critical Infrastructure

White House Executive Order (EO) 13636[3] tasked the Director of the National Institute of Standards and Technology (NIST) to "lead the development of a framework to reduce cyber risks to critical infrastructure (the ''Cybersecurity Framework'')." The "Framework for Improving Critical Infrastructure Cybersecurity" (the "Cybersecurity Framework" as called for in EO 13636) [4, 5] was published in February 2014, and the important work of integrating the Cybersecurity Framework into organizational operations is well underway in many industries. The Cybersecurity Framework provides an approach to analyzing cybersecurity risk, enabling enterprises to understand their cybersecurity challenges, and selecting appropriate mitigation strategies. The Cybersecurity Framework emphasizes the risk management process for cybersecurity by stating:

"The Framework focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes."

The Cybersecurity Framework also provides a common taxonomy for discussing cybersecurity activities within an organization (e.g., between a Chief Information Security Officer and the Board of Directors) and between organizations (e.g., organizations that rely on cybersecurity capabilities with other partnering organizations). When used in conjunction with the concept of Cybersecurity Framework's Framework Implementation Tiers or other methods of measuring progress, such as maturity modeling, the Cybersecurity Framework also provides a way for an organization to measure the progress of its cybersecurity activities over time and to benchmark against other organizations. It can also be used to communicate cybersecurity capabilities to auditors, regulators, and other types of assessors.

The Cybersecurity Framework breaks cybersecurity into five Functions that, taken together, provide a "high-level, strategic view of the lifecycle of an organization's management of cybersecurity."[6] The five Functions are: Identify, Protect, Detect, Respond, and Recover. Each of the Functions are further divided into Categories and Subcategories.

2.2. Cybersecurity Risk in the MBLT Enterprise

The Department of Homeland Security designated the energy and transportation sector as two of the 16 critical infrastructure sectors to our nation.[7] These sectors include both oil and natural gas, with MBLT operations representing significant activities within the subsectors.

---

[3] Executive Order – *Improving Critical Infrastructure Security*, February 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[4] http://www.nist.gov/cyberframework/

[5] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, *Version 1.0*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[6] Cybersecurity Framework, p. 4

[7] https://www.dhs.gov/critical-infrastructure-sectors

2.2.1. Information Technology (IT) and Operational Technology (OT)

Although MBLT operations have not always relied on combined IT and OT processes, they are increasingly evolving towards a combined reliance. This introduces new cybersecurity risks that MBLT operators are working to manage. While managing cybersecurity risks is equally important to IT and OT processes, implementation of risk management techniques varies considerably due to safety concerns and operational differences between the two. Appropriate security controls must be in place for IT to reliably support processes such as human resources, training, and business communication. Likewise, OT security controls must be in place to reliably support and ensure safety and security of the storage, transfer, pressure monitoring, vapor monitoring, emergency response, and spill mitigation systems. It is only through integrated assessment, mitigation, and recovery planning against cybersecurity threats in both IT and OT systems that the cybersecurity risks to MBLT can be appropriately managed as part of an integrated risk management system.

MBLT is part of a complex and sophisticated supply chain in the oil and natural gas (ONG) industry with interdependencies between various types of organizations and systems. The MBLT mission area covers a blend of enterprise IT and OT. Both technologies must provide the proper data inputs so Mission Objectives and needs are satisfied in a safe and secure manner. Interdependencies between IT and OT can create multiple risks for the enterprise that must be managed.

2.2.2. IT Cybersecurity Risk

Risk assessment is a key component of IT cybersecurity. Cybersecurity risk is now a key element of corporate risk management because of the extensive interdependence of IT and OT systems.

In many enterprises cybersecurity risk management has evolved from a periodic static compliance assessment to a dynamic real-time continuous monitoring and assessment of IT systems. Each level of the assessment provides metrics that decision makers can use to identify threats and determine which mitigation strategies to pursue. Mitigation techniques range from updates to antivirus tools and forced patching of business computers, to sophisticated intrusion detection systems, to real-time sharing of information threat risks.

2.2.3. OT Cybersecurity Risk

OT typically refers to the systems, processes, procedures, equipment, communication, controls, alarms, and devices that monitor and control an industrial process in a manner that is safe and efficient. The processes involved in MBLT are supported by OT.

Originally, OT was a distinct domain found in industrial plants, power and communications networks, manufacturing facilities, mining, drilling, and production. Many OT systems were purpose-built, stand-alone systems with manually operated controls. Safety procedures were put in place for such an environment. The terms Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) were created to describe these systems as they became automated with analog and digital controls.

During the last fifteen years, SCADA/ICS systems have begun to use technologies, networks, and component designs that incorporate general-purpose computers, communications, and interconnected networks. The introduction of these capabilities provided simplification, cost reduction, and increased the efficiency of the processes they control. However, the open and interconnected systems that provide these benefits also introduce cybersecurity risk to the processes.

Threats surrounding SCADA/ICS systems continue to be of concern to OT professionals.[8] Exchange and validation of information about threats is supported by the ICS Cyber Emergency Response Team (ICS-CERT)[9] of the Department of Homeland Security (DHS). ICS-CERT provides alerts, advisories, and reports. It also has a series of standards and references[10] and conducts assessments[11].

In addition to its work on Cybersecurity Framework implementation, the Department of Energy (DOE) has developed the Cybersecurity Capability Maturity Model (C2M2) program which maps cybersecurity capability to maturity levels. More information regarding DOE cybersecurity programs is provided in Appendix C.

2.3. Regulatory Context

The USCG is responsible for overseeing multiple mission areas regarding the navigable waters of the United States, which includes the regulation of:

- facilities transferring oil or hazardous material in bulk (33 CFR 154)
- oil or hazardous material pollution prevention regulations for vessels (33 CFR 155)
- oil and hazardous material transfer operations (33 CFR 156)[12]

[8] Department of Energy, National SCADA Test Bed, http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed

[9] Department of Homeland Security, DHS, Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov/

[10] DHS, ICS-CERT Standards and References, https://ics-cert.us-cert.gov/Standards-and-References

[11] DHS, ICS-CERT Assessments, https://ics-cert.us-cert.gov/Assessments

[12] Appendix B provides the details of the cybersecurity evaluation of these regulations.

In support of those mission areas, the USCG created a number of safety regimes outlined in the Code of Federal Regulations (CFR). Over the last several years it has come into question whether the emerging cybersecurity threats can have a direct or indirect impact on safety in those mission areas. To address this concern, the USCG has engaged in several ways:

- development of a USCG Cybersecurity Strategy[13]
- cybersecurity-related interviews with Federal Advisory Committees[14, 15] concerned with safety and security matters
- engagement with industries that participate in its mission areas regarding their views on cybersecurity threats, as well as appropriate architectures, tools, techniques, and systems to mitigate those threats

The USCG consulted NIST regarding its work on the Cybersecurity Framework, and as a result of those discussions determined that an industry-focused Cybersecurity Framework Profile should be created. NIST personnel who oversaw the development of the Cybersecurity Framework along with personnel from its NCCoE [16] have worked with industry and the USCG to develop Cybersecurity Framework Profiles that can be used by industry to assess their cybersecurity posture and readiness regarding several USCG mission areas.

The USCG is working with industry to develop these voluntary industry-focused Profiles to mitigate risks in their joint mission areas. The USCG determined the first industry-focused Profile should address MBLT. Specifically, MBLT is regulated under 33 CFR Parts 154, Facilities Transferring Oil or Hazardous Material in Bulk, 33CFR Part 155, Oil and Hazardous Material Pollution Prevention Regulations for Vessels, and 33 CFR 156, Oil and Hazardous Material Transfer Operations. Other mission areas regulated under 33 CFR 104-106 to be evaluated in future Profiles include maritime cybersecurity for passenger vessels, cargo vessels, navigation, and offshore facilities.

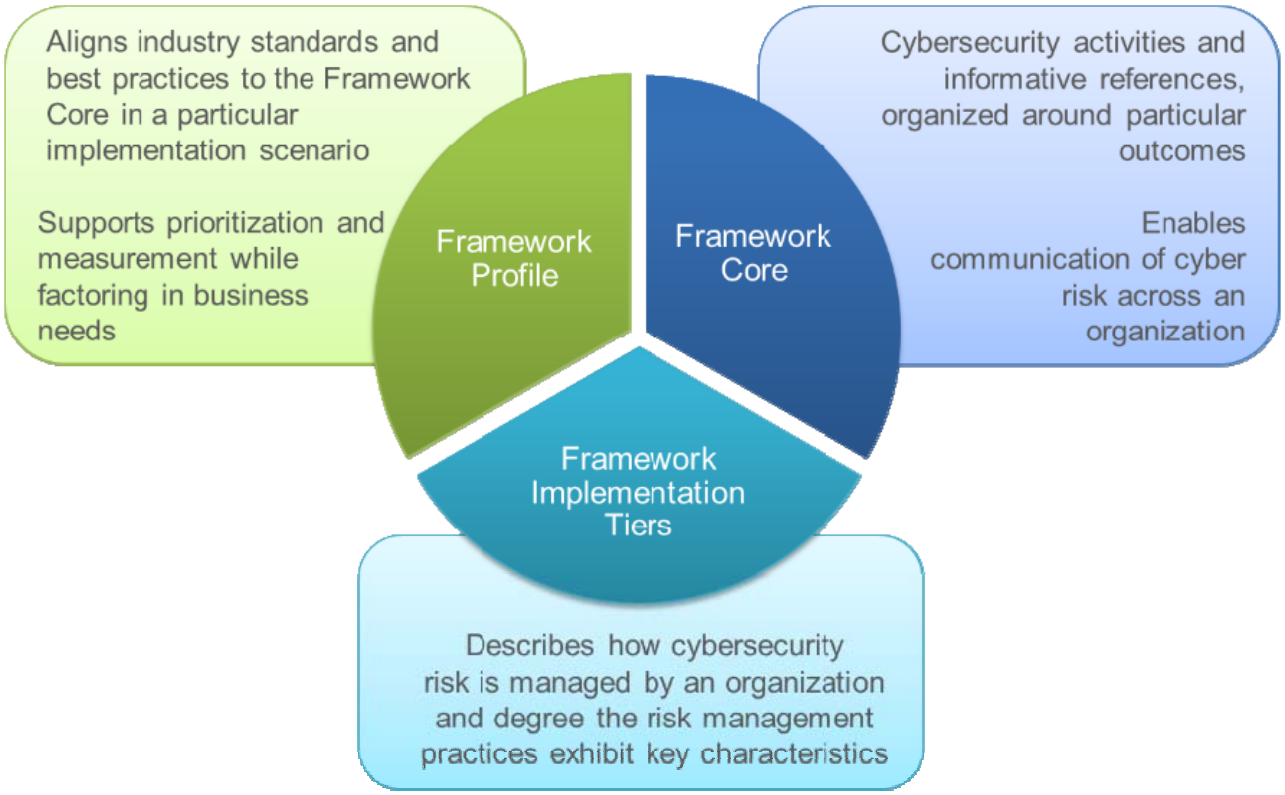
[13] *United States Coast Guard Cyber Strategy*, June 2015, https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf
[14] United States Coast Guard, Notice of Federal Advisory Committee Meeting. See especially New Business item 2.a. Cybersecurity on the Outer Continental Shelf https://www.federalregister.gov/articles/2015/03/20/2015-06413/national-offshore-safety-advisory-committee-meeting
[15] United States Coast Guard, National Maritime Security Advisory Committee; Meeting, Notice of Federal Advisory Committee Meeting. See especially Agenda of Meeting Day 1 (1) Coast Guard Cyber Security Strategy https://www.federalregister.gov/articles/2015/08/25/2015-20953/national-maritime-security-advisory-committee-meeting
[16] National Cybersecurity Center of Excellence, https://nccoe.nist.gov/

3. Using the Cybersecurity Framework

3.1. Cybersecurity Framework Basic Elements

The components of the Cybersecurity Framework, identified in Figure 3-1, include the Framework Core, Implementation Tiers, and Profiles.

Figure 3-1. Elements of the Cybersecurity Framework

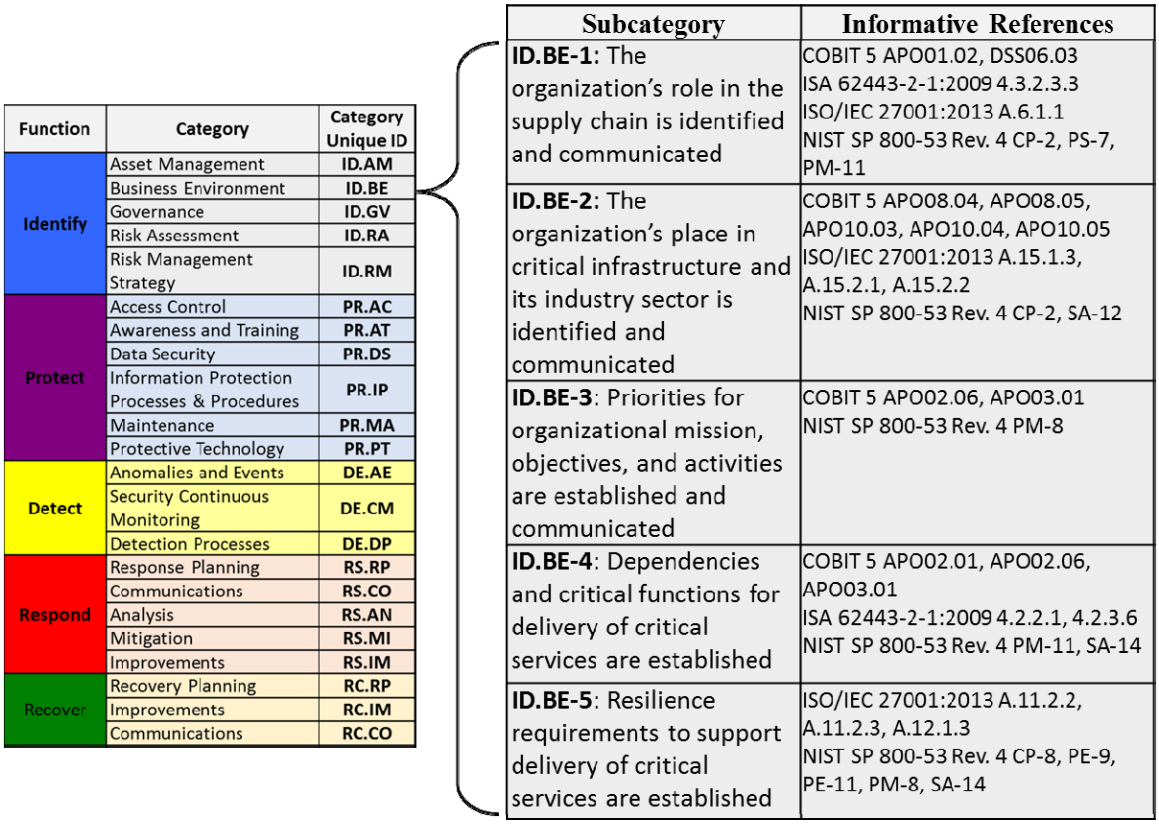


The Framework Core is structured into five Functions that identify the key cybersecurity outcomes identified to manage cybersecurity risk:

- **Identify** – develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- **Protect** – develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
- **Detect** – develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- **Respond** – develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- **Recover** – develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

As seen in Figure 3-2, each of these Functions is color-coded, and is further divided into Categories and Subcategories. Each Category has a Category Unique ID. Each Subcategory has a textual description and Informative References.

Figure 3-2. Functions, Categories, and Subcategories of **the Cybersecurity Framework**



Function	Category	Category Unique ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	COBIT 5 APO01.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.3.3 ISO/IEC 27001:2013 A.6.1.1 NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	COBIT 5 APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 ISO/IEC 27001:2013 A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 CP-2, SA-12
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	COBIT 5 APO02.06, APO03.01 NIST SP 800-53 Rev. 4 PM-8
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	COBIT 5 APO02.01, APO02.06, APO03.01 ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 NIST SP 800-53 Rev. 4 PM-11, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14

The Functions in the Framework Core essentially ask organizations to consider questions such as:

- What processes and assets need protection?
- What safeguards are available?
- What techniques can identify incidents?
- What techniques can contain impacts of incidents?
- What techniques can restore capabilities?

3.2. Cybersecurity Framework Profiles

Overview of Profiles

As an organization determines how to use the Cybersecurity Framework Core to assist in managing its cybersecurity risks, it can develop an organization-specific Profile to map its current state and a desired future state based on the organization's mission.

The following excerpt from the Cybersecurity Framework describes Profiles:

"Through use of the Profiles, the Framework will help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources.

. . . A Framework Profile ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state)."

Tailoring a Profile

Profile development tailors the Cybersecurity Framework to focus on the cybersecurity areas of particular concern to an industry, organization, or functional area as identified through its risk management processes. By evaluating the elements of the Cybersecurity Framework against a particular mission, a Profile is created that shows priorities based on evaluation of the mission against the Cybersecurity Framework Functions, Categories, and Subcategories. There are a number of ways to view a Profile. These include:

- a customization of the Cybersecurity Framework Core for a given industry, subsector, or organization
- a fusion of business/mission logic and cybersecurity outcomes
- an alignment of cybersecurity requirements with operational methodologies
- a basis for assessment and expressing target state
- a decision support tool for cybersecurity risk management

Implementing and Leveraging Profiles in Organizations

The Cybersecurity Framework and Profiles created with it provide a consistent way to discuss security objectives and activities in reader-friendly terminology that is consumable for multiple roles – from executives to technical implementers. Within organizations, benefits include describing how security investments will be used to a Board of Directors, and measuring progress in meeting cybersecurity objectives year over year. Advantages provided by industry-focused Profiles include defining consistent priorities across a sub-sector, and enabling conversations by discussing security activities using consistent terminology. Industry-specific Profiles are intended to:

- minimize future work by each organization
- decrease the chance that organizations accidentally omit a requirement
- encourage consistent analysis of cybersecurity-risk in the MBLT environment
- align industry and USCG cybersecurity priorities

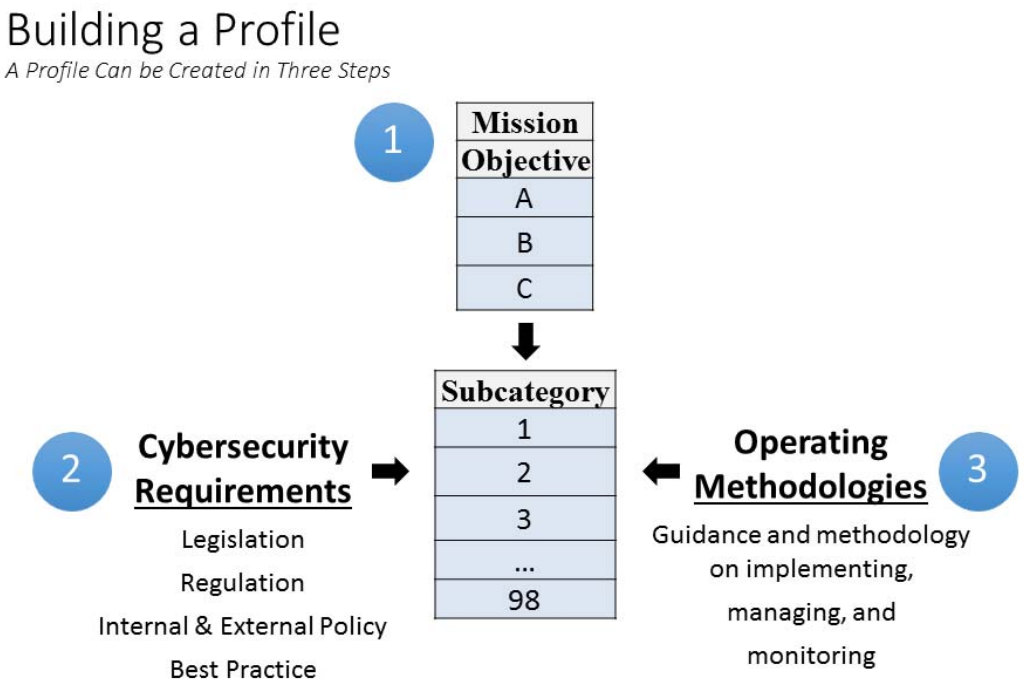
Organizations that are part of an industry or sub-sector that has one or more industry-focused Profile generally use those industry-focused Profiles to inform decisions made when constructing their organization-focused Profile and measuring progress.

3.3. Developing a Profile

As shown in Figure 3-3, there are three steps to developing a Cybersecurity Framework Profile:

1. describe and map Mission Priorities and Objectives with awareness of the regulatory environment
2. review Mission Objectives at the Subcategory level in light of cybersecurity requirements
3. consider the Subcategories in light of operating methodologies to develop guidance for implementing, managing, and monitoring the selected Subcategories and document decisions made regarding prioritization

Figure 3-3. Mapping Mission Priorities



As an organization transposes its Mission Objectives to cybersecurity requirements, there are a series of guiding questions that inform the process. They include:

- What threats exist to achieving those Mission Objectives?
- What sort of damages can it cause when those Mission Objectives are disrupted?
- What are your most important assets for a given Mission Objective?
- Where does physical infrastructure affect cybersecurity infrastructure and vice versa?

An organization should also be aware of statutory and policy requirements that may have a security or safety dimension. These can be affected by cybersecurity risk or create risks downstream.

As the organization reviews operating methodologies[17], it should ask:

- Is our current list of operating methodologies accurate?
- Do we have any additional operating methodologies?

The output of this three step process informs the prioritization of Cybersecurity Framework Subcategories in the resulting Profile.

3.4. Advantages of Developing a Profile

According to the developers of the Cybersecurity Framework, organizations gain the following advantages by developing a Profile:

- compliance reporting becomes a byproduct of running your security operation
- adding new security requirements is more straightforward
- adding or changing operational methodology is less intrusive to ongoing operations
- identifying cybersecurity gaps regarding technology, processes, and people

Each organization implementing this Profile has the ability to map its current capabilities to the MBLT CFP. This can support a gap analysis to assist the organization in attaining the desired state of full implementation of the MBLT CFP. Further, the MBLT CFP can be tailored by the organization to identify an organizationally-specific desired 'to be' state. This process allows an organization to use the gap analysis to drive budget, schedules, and resource allocations as the organization plans for achieving the desired state. This Profile is best leveraged as part of the IT/OT planning process in order to develop an organized, step-wise plan and budget allocations to resource the evolution from the 'as is' state to the desired 'to be' state.

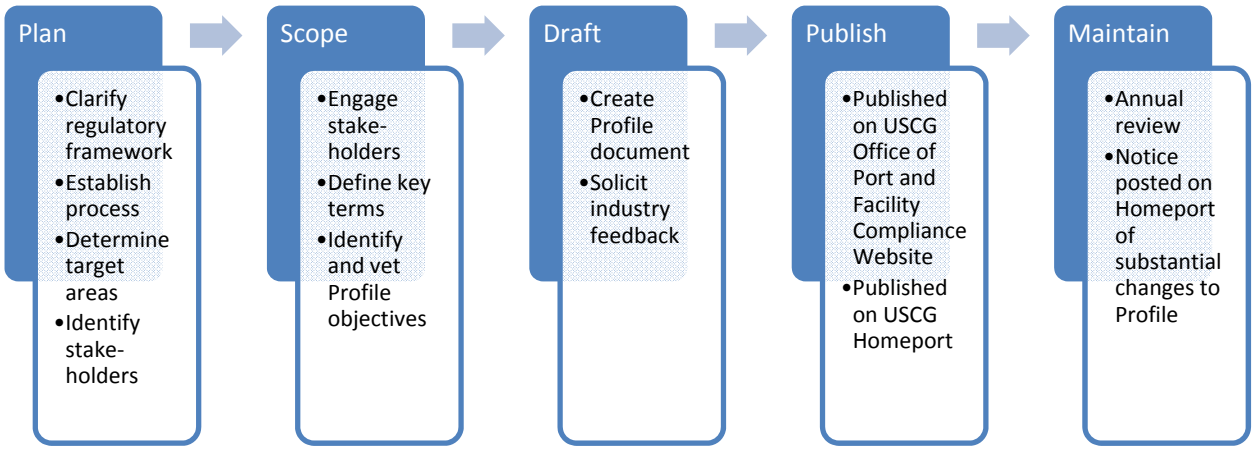
4. The MBLT CFP for Industry

While Section 3 discusses Cybersecurity Framework Profiles generally, this section discusses the process to create and implement an industry-specific MBLT CFP to add a cybersecurity dimension to the facility and vessel security plans required under 33 CFR 104-106. This section describes the steps in the Profile development process, the regulatory and statutory foundations for the MBLT CFP, and governance.

4.1. Overall Process to Create this Profile

Figure 4-1, MBLT CFP Development Process, shows the process followed to develop the MBLT CFP.

Figure 4-1. MBLT CFP Development Process



Plan

The Plan phase involved the development of an awareness of the regulatory framework surrounding MBLT operations. The existing regulatory framework is ambiguous regarding cybersecurity in MBLT operations. However, MBLT operations are generally well-documented in the regulatory guidance provided by the USCG in the CFR. Once clarity on the regulatory framework was achieved, the overall objectives were refined and the process for proceeding with Profile development was established. The Plan phase also included activities to identify operational and mission areas to target, and to develop a team of stakeholders.

Scope

The Scope phase involved outreach and engagement with stakeholders—primarily owners and operators in the industry. Avenues for engaging industry members included the Cybersecurity Subcommittee of the USCG National Offshore Safety Advisory Committee (NOSAC) Federal Advisory Committee, trade associations, targeted cybersecurity conferences, and those identified through other research. The latter included a review of materials from the DOE, ICS-CERT, the American Petroleum Institute (API), American Fuel and Petrochemical Manufacturers (AFPM), the American Water Works Association, and attendance at several industry conferences. A series of in-person discussion sessions were held with stakeholders to develop the Mission Objectives defined in Section 6.1 and identify the priority Functions within the Cybersecurity Framework for each of the Mission Objectives. As part of this process, the Cybersecurity Framework itself was shared with industry members who typically focus on

the safety regimes, monitoring, inspection, and testing of MBLT operational environments. Through this step, the Mission Objectives and their priorities were further refined.

Draft

The Draft phase included the creation of the raw Profile, its development and refinement, and incorporation of revisions in response to industry feedback. The MBLT Profile was further developed by identifying and prioritizing the Cybersecurity Framework Subcategories in support of each Mission Objective. An initial working version was shared with industry personnel, the NOSAC Cybersecurity Subcommittee, and trade association cybersecurity committee members. A revised draft was prepared for sharing based on feedback received during the NIST Cybersecurity Framework Workshop in April 2016.

Publish

In the Publish phase, the USCG will release the Profile to the broader maritime community. The enterprises involved in MBLT operations are recommended to incorporate the Profile into their enterprise risk management processes and document those results..

Maintain

In the Maintain phase, the Profile will be monitored for usefulness. Any gaps will be identified and recorded. Over time, updates to the Profile may be adopted based on the information gathered in this phase. As part of the maintenance process the USCG will continue its dialog with industry and those regulated under MBLT regulations. As regulation, policy, and technical capabilities change, this Profile will need to be reviewed and possibly revised under whatever governance process is ultimately determined.

4.2. Activities to Date

An initial set of meetings was held during the Scope Phase to determine the process for identifying the cybersecurity risks in an MBLT environment. A number of Mission Objectives were identified and prioritized by a USCG and industry team assisted by NIST personnel. The team then met with representatives from the Cybersecurity Subcommittee of the NOSAC at their September 2015 meeting in Houston, TX. In addition to a briefing about the approach used by NIST at the subcommittee meeting, a group gathered the next day to conduct a validation and mapping exercise against the Cybersecurity Framework. During this session, Mission Objectives were validated and Cybersecurity Framework Functions were prioritized according to the Mission Objectives. Those assembled initially broke into several teams to evaluate the priorities and then came together to create a consensus view of the priorities.

Next, the USCG and NCCoE spent several days refining the identified priorities at the Cybersecurity Framework Subcategory level. This mapping was then shared back with the NOSAC Cybersecurity Sub-committee as well as representatives of the API and AFPM. A review of each of the mission mappings to the Cybersecurity Framework Subcategories was conducted during a series of conference calls with the API/AFPM group. A higher level session was also held at the API Cybersecurity Conference in Houston, TX, in early November 2015.

During the Draft phase, the USCG and NCCoE drafted the MBLT CFP based on the industry input received during the Scope phase. The team discussed an early draft with the NOSAC Cybersecurity Subcommittee during a work session held in February 2016 in Houston, TX. The USCG solicited additional feedback internally, through its engagement with various ONG trade associations, and at a dedicated session of the Cybersecurity Framework Workshop held in April 2016 in Gaithersburg, MD, to validate the direction of the document. The team further refined this Profile based on internal and external feedback to produce this version. As part of this process, the NCCoE has delivered this initial version to the USCG for industry use.

4.3. Profile Foundations

The following authorities and resources form the basis for the MBLT CFP:

- United States Coast Guard, Maritime Cybersecurity Standards, 78883 [2014--30613], https://www.federalregister.gov/documents/2014/12/18/2014-29658/guidance-on-maritime-cybersecurity-standards [accessed 9/14/16]
- United States Coast Guard (USCG) and Code of Federal Regulations (CFR) (33 CFR 154-156) requirements, http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title33/33cfr154_main_02.tpl [accessed 9/14/16]
- International Convention for the Prevention of Pollution from Ships (MARPOL), http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-(MARPOL).aspx [accessed 9/14/16]
- International Convention for the Safety of Life at Sea (SOLAS), http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx [accessed 9/14/16]
- Executive Order no. 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013, (The White House), https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [accessed 9/14/16]
- National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* , February 12, 2014. https://www.nist.gov/cyberframework [accessed 9/14/16]
- Cybersecurity Capability Maturity Model, v 1.1, February 2014. http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program [accessed 9/14/16]

Additionally, the U.S. maritime and ONG industry used several cybersecurity standards and guidance documents to establish cybersecurity/cyber-risk policies and procedures, including the Cybersecurity Framework and USCG regulations listed above. The specific standards and processes used vary by company. The following is a sample of those cybersecurity standards and guidance:

- American National Standards Institute, *Security for Industrial Automation and Control Systems*, ANSI/ISA 99.

- American Petroleum Institute, *Security Risk Assessment Methodology*, API –STD-780.
- Center for Internet Security (CIS) 20: *Critical Security Controls for Effective Cyber Defense.*[18]
- International Electrotechnical Commission, *Power Systems Management and Associated Information Exchange - Data and communications security*, IEC 62351.
- International Maritime Organization, *Ensuring Security in and Facilitating International Trade, Measures Toward Enhancing Maritime Cybersecurity* (as submitted by Canada), IMO Publication 39/7, 10 July 2014.
- International Maritime Organization, *International Ship and Port Facility Security (ISPS) Code* framework. Implemented through the Safety of Life at Sea (SOLAS) Treaty as implemented by the Maritime Transportation Security Act of 2002.
- International Maritime Organization, MSC.1/Circ.1526 Interim Guidelines On Maritime Cyber Risk Management.
- International Organization for Standardization, *Security Management Systems for the Supply Chain; Best Practices for Implementing Supply Chain Security, Assessments and Plans - Requirements and Guidance*, ISO 28001:2007, 2007.
- International Organization for Standardization, *Information Technology - Security Techniques - Information Security Management Systems – Requirements*, ISO/IEC 27001:2013, 2013.
- International Organization for Standardization*, Information Technology - Security Techniques - Code of Practice for Information Security Controls*, ISO/IEC 27002:2013, 2013.
- International Organization for Standardization, *Guidelines to Cybersecurity*, ISO 27032.
- International Society for Automation, Security for Industrial *Automation and Control Systems Security Standard of Good Practice for Information Security*, ISA/IEC 62443.
- NIST 800-53, Rev 4: *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST Special Publication 800-53, Revision 4, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2013, 462pp. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf [accessed 9/12/16]
- North American Electric Reliability Council (NERC), Critical Infrastructure Protection (CIP) Version 5.[19]
- SANS Institute, *The Industrial Control System Cyber Kill Chain*, October 2015. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297 [accessed 9/14/16].

4.4. Governance

The USCG will annually review this Profile and will inform industry of substantial changes with a notice on Homeport and the Office of Port and Facility Compliance website. Changes to this Profile may be informed by legislation, policy changes, major event and response, and technology changes.

[18] https://www.cisecurity.org/critical-controls/

[19] NERC CIP Version 5 Standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. NERC CIPv5 Implementation Study Final Report, October 2014, http://www.nerc.com/pa/CI/tpv5impmntnstdy/CIPv5_Implem_Study_Final_Report_Oct2014.pdf

5. Roadmap for Organizations Using the MBLT CFP

The MBLT CFP is intended to lend consistency to the definition of Mission Objectives and prioritization of the relevant cybersecurity activities conducted by organizations in the industry, regardless of variations in the unique characteristics in organizations, including demographics, individual missions, and resources.

5.1. Cybersecurity Profile Development and Use for MBLT Organizations

The Cybersecurity Framework describes a seven-step process for an organization to develop and use the Cybersecurity Framework for planning and risk mitigation.[20] The steps are:

- Step 1: Prioritize and Scope
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- Step 5: Create a Target Profile
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan

This document defines the Profile for MBLT per Step 3. This MBLT Profile provides an industry view of cybersecurity priorities for the MBLT subsector of the ONG industry. Organizations may use this Profile as input into their activities during Step 5 above, Create a Target Profile, as well as certain elements of Step 3, Create a Current Profile. The MBLT Profile acts as a starting point for organizations to review and adapt their risk management processes when creating their organization's Target Profile. Once an organization's Target Profile is created, it uses the organizational Target Profile to perform Steps 6 and 7 to address its specific priorities.

5.2. Process to Incorporate the MBLT Profile in Organizations

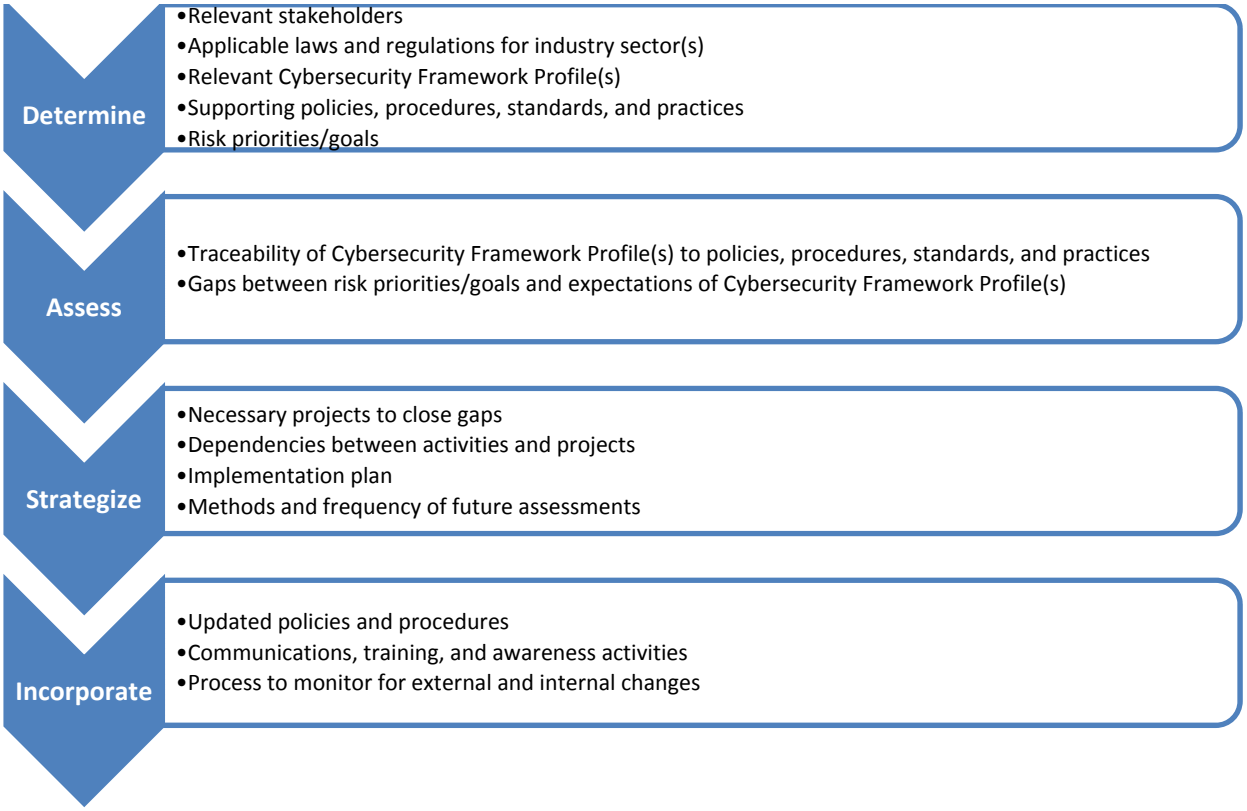
As organizations utilize this Profile and complete the steps outlined above, they should integrate implementation of the Profile into their enterprise. Each organization, with its understanding of policy drivers, relevant standards, and other Cybersecurity Framework Profiles, should adapt this Profile to meet its needs regarding compliance with regulations and best practices for MBLT operations. All of this should be done within the context of the Cybersecurity Framework's guidance.

Figure 5-1 provides a representative example of the processes an organization may follow to evaluate the MBLT Profile and incorporate it into the organization's cybersecurity program. While the diagram and this discussion focuses mostly on incorporating a Profile into organizational practices, these activities are most effective when incorporated into the organization's overall cybersecurity strategy, and not as a stand-alone Profile exercise. Organizations will typically need to start by determining who the key stakeholders are, what drives (or should be driving) their cybersecurity decisions, and what their risk priorities and goals are. Once those foundational activities have been conducted, the organization

[20] For energy sector organizations, readers should also be mindful of the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability document, "*Energy Sector Cybersecurity Framework Implementation Guidance*" (January 2015).

can assess where they are against where they would like to be, using the inputs identified in the previous step (e.g., the MBLT Profile). The outcomes of the assessment inform the next step, developing the strategy and specific plans for implementing the MBLT Profile (and other cybersecurity initiatives identified) within the organization. Making the necessary changes within the organization occurs during the incorporate phase.

Figure 5-1. Steps to Applying the Profile to Your Organization



The goal of these steps is to identify and mitigate gaps discovered during the process. Such mitigation will assist the organization in increasing capabilities and resilience.

6. Mission Mapping, Cybersecurity Framework Functions, Categories, and Subcategories

The MBLT Profile is a customization of the Cybersecurity Framework for the MBLT industry subsector based on input from subject matter experts on existing processes, cybersecurity capabilities and operational technology. It fuses business and mission logic in the implementation of MBLT regulations. It aligns cybersecurity with MBLT operational methods. As it is utilized by MBLT organizations, it can supplement their existing cybersecurity risk management processes.

6.1. MBLT CFP Structure

The MBLT CFP uses the Framework Core, which is built around five Functions: Identify, Protect, Detect, Respond, and Recover. Each of these Functions is broken into Categories and Subcategories that describe expected outcomes of cybersecurity activities. The Framework Core is described in Section 3.1.1 of the Cybersecurity Framework.

Implementing Cybersecurity Framework Profiles in a way that is relevant to industry depends on defining Mission Objectives that are meaningful in the context of industry activities. In order to align the Cybersecurity Framework with the mission needs of MBLT operations, the USCG worked with industry to define the key Mission Objectives that shape cybersecurity activities. These Mission Objectives provide the necessary context for identifying and managing cybersecurity risk. Cybersecurity practices for MBLT operations rely on the eight Mission Objectives defined in the following table.

Table 6-1. MBLT Mission Objectives

Mission Objective	Description
1: Maintain Personnel Safety	Cybersecurity-effect on process control systems impacts personnel safety. Organizations should: • manage risks to the organization and industry using a structured process • identify and train personnel on interdependence of cybersecurity with operational responsibilities • implement Detect/Respond/Remediate activities where cybersecurity adversely affects personnel safety
2: Maintain Environmental Safety	Cybersecurity-effect on process control systems impacts environmental safety. Organizations should: • manage risks to the organization and industry using a structured process • identify and train personnel on interdependence of cybersecurity with operational responsibilities • manage prominent and increasing role of automated systems in maintaining quality control of product during safe transport • implement Detect/Respond/Remediate activities where cybersecurity adversely affects environmental safety

Mission Objective	Description
3: Maintain Operational Security	Cybersecurity-effect on security control systems impacts operational safety and security. Organizations should: • manage risks to the organization and industry using a structured process • identify and train personnel on interdependence of cybersecurity with operational responsibilities • manage prominent and increasing role of automated systems in maintaining physical control of infrastructure • implement Detect/Respond/Remediate activities where cybersecurity adversely affects safety and security
4: Maintain Preparedness	Cybersecurity-effect on systems readiness that can impact operations including maintenance, documentation and testing for safety and security. Organizations should: • develop systems and train personnel to integrate cybersecurity-impacts on resilience in maintaining mission assurance • implement resilience-aware activities including o risk mitigation procedures o ongoing situational awareness o backup/resilience/fail-safe modes o regular preventive maintenance
5: Maintain Quality of Product	Cybersecurity-effect on systems can impact product quality, maintenance, and systems monitoring. Impacts can include loss of confidentiality and integrity such as disclosure of status information or test results to unintended parties. Organizations should: • develop systems and train personnel to acknowledge potential cybersecurity risk vectors in maintaining product quality • plan for quality measures including: o testing o preventive maintenance o remediation o ongoing situational awareness • manage prominent and increasing role of automated systems in maintaining control of product during safe transport.

Mission Objective	Description
6: Meet HR Requirements	Cybersecurity-effect (security and privacy) on operational systems impacting security and trust of personnel and their information. Organizations should: • ensure appropriate governance, plans, procedures and oversight of connected HR systems and data including roles of employee managers in training and awareness • understand risks, identify and train personnel on interdependence of cybersecurity with operational responsibilities and connections to source HR systems • implement procedures to protect data in systems that contain personnel information • implement Detect/Respond/Remediate activities where cybersecurity adversely affects personnel or personnel data.
7: Pass Required Audits/Inspections	Developing systems and training personnel to demonstrate readiness and execution of established plans. Organizations should: • review plans and conduct in-person inspections via various means including: o automated/cybersecurity interface testing o sensor testing o backup/resilience process evaluation o plan and testing of data exchange/reporting methods • ensure confidentiality of sensitive data, plans, and procedures
8: Obtain Timely Vessel Clearance	Assure cybersecurity dimension of systems that can impact readiness and operational preparedness. Organizations should: • demonstrate and share documents, data and other items to assure safe and secure entry into a port environment • ensure confidentiality of sensitive data, plans, and procedures, particularly personnel data and documents

The capabilities of organizations vary widely. Subcategories from the Cybersecurity Framework are prioritized for each MBLT Mission Objective, where relevant, to identify those that most directly support industry Mission Objectives. In order to help organizations prioritize and allocate resources most effectively, the priority Subcategories are designated as “High Priority Subcategories” and “Moderate Priority Subcategories.” Section 6.2 provides a summary table of the priority Subcategories specified in the MBLT CFP. While the MBLT CFP specifies the most critical Categories and Subcategories, other Cybersecurity Framework Categories and Subcategories would also be included and active in the operational systems interfacing with MBLT operations. Organizations should also be mindful that MBLT operations are controlled by strict guidelines and procedures outlined in regulatory guidance.

Appendix A provides the full detailed MBLT CFP. In addition to the information provided in Section 6.2, the detailed MBLT CFP provides a description of how the Mission Objectives relate to each Cybersecurity Framework Function, the rationale for specifying each High Priority Subcategory, and Optional Resources, which include Informative References from the Cybersecurity Framework and industry-specific additions, such as related C2M2 practices.

6.2. Summary of Priority Subcategories Identified

Organizations should strive to conduct activities in support of all relevant Subcategories in the Cybersecurity Framework. This MBLT CFP recognizes that expectation and further specifies a subset of Cybersecurity Framework Subcategories to help each organization prioritize implementation of any Subcategories they are not yet addressing. Organizations that have already addressed all relevant Subcategories may choose to incorporate this MBLT CFP as input into future prioritization and improvement activities. Subcategory selections are included for each of the eight Mission Objectives required to conduct MBLT operations in a more secure manner.

From the perspective of the USCG and industry participants that contributed to development of this Profile, some Subcategories are more critical than others to supporting the cybersecurity needs of the Mission Objectives. To that end, Subcategories are divided into three types for the purposes of the MBLT CFP[21]:

- **High Priority**: the most critical Subcategories for enabling a given Mission Objective in a more secure manner
- **Moderate Priority**: Subcategories that, while not as urgent as the High Priority Subcategories, must also be addressed in order to implement a given Mission Objective in a more secure manner
- **Other Implemented Subcategories**: Subcategories that are important for each Mission Objective and the organization overall, but not the most critical for organizations that have not yet addressed the priority Subcategories

High and Moderate Priority selections for each Mission Objective are focused on the outcomes the USCG sees as most important, and may not always include interdependencies. For some Functions, only Other Implemented Subcategories were specified. In others, Subcategories are specified as High or Moderate Priority, but the interdependencies in other Functions were not selected. In these cases, the USCG made a judgment call to distinguish the most impactful Subcategories in an effort to avoid the challenge of all Subcategories or no Subcategories being viewed as most important. Eventually, MBLT operations organizations should address all Subcategories. The intent of the Profile is to suggest areas of focus for organizations that are in earlier phases of implementing their cybersecurity programs. Table 5-2 provides a summary of Subcategory priorities by Mission Objective. This is further defined in Appendix A, which provides the full detailed MBLT CFP.

[21] The prioritization of Subcategories may vary between Profiles for ONG and other industries, depending on Mission Objectives and other relevant factors to other Profiles.

Risk management programs and cybersecurity decisions vary in accordance with the unique needs of each organization. Priorities, emphases, and approaches to addressing Subcategories may differ from organization to organization. For that reason, the MBLT CFP does not dictate how or in what order organizations address the High and Moderate Priority Subcategories. This leaves the approach used to pursue implementation of the Subcategories up to organizations individually. The following are examples of ways organizations may decide to prioritize their implementation:

- all High Priority items, followed by all Moderate Priority items, then Other Implemented Subcategories
- by Mission Objective, starting with the ones that are most impactful to that particular organization
- by Framework Core element, i.e., focusing on a single Function, Category, or Subcategory across all Mission Objectives
- Subcategories the organization finds easiest to address

Other approaches may be more appropriate for a given organization. Organizations that have not yet addressed all relevant Subcategories in the Cybersecurity Framework have the flexibility to prioritize in whatever way makes most sense for their unique risk posture, including addressing Other Implemented Subcategories first.

Regardless of the method used, organizations should describe their current state in an 'as is' Profile and with their own review of this document as an initial 'to be' Profile. This will facilitate the ability to conduct a gap analysis on what measures should be added to fill in the needed subcategories. It can also frame the discussion with the organization's IT governance and IT investment functions. Organizations can then use the Framework Implementation Tiers described in the Cybersecurity Framework to assess progress.

Table 6-2. Summary of Subcategory Priorities by Mission Objective

Function	Category	Subcategory	Mission Objectives ●●● = High Priority, ●● = Moderate Priority, ● = Other Implemented Subcategories							
			1	2	3	4	5	6	7	8
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives	**ID.AM-1**: Physical devices and systems within the organization are inventoried	●	●●●	●	●	●●	●	●	●
		ID.AM-2: Software platforms and applications within the organization are inventoried	●	●●	●	●	●	●	●	●
		ID.AM-3: Organizational communication and data flows are mapped	●	●	●	●	●●	●	●	●

	and the organization's risk strategy.	**ID.AM-4:** External information systems are catalogued	●	●	●	●	●	●	●	●
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	●	●●●	●	●	●●●	●	●	●
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	●	●	●	●	●●	●	●	●
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	●	●	●	●	●	●	●	●
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	●	●	●	●	●	●	●	●
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	●	●	●	●	●	●	●●	●●
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	●	●	●	●	●	●	●●	●●●
		ID.BE-5: Resilience requirements to support delivery of critical services are established	●	●	●	●	●	●	●●●	●

	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	●	●	●	●	●	●●	●	●
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	●	●	●	●	●	●●	●	●●
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	●	●	●	●	●	●●●	●●●	●●●
		ID.GV-4: Governance and risk management processes address cybersecurity risks	●	●	●	●	●	●	●●	●
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	●●●	●●	●●	●●	●●	●	●	●
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	●●	●	●	●	●	●	●	●
		ID.RA-3: Threats, both internal and external, are identified and documented	●●	●●	●	●	●	●	●	●
		ID.RA-4: Potential business impacts and likelihoods are identified	●●	●●	●	●	●	●	●	●
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	●●●	●●	●●●	●●●	●●●	●	●	●
		ID.RA-6: Risk responses are identified and prioritized	●●●	●●	●	●	●	●	●	●

	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	●●●	●	●	●	●	●	●	●
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	●●	●	●	●	●	●	●	●
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	●●	●	●	●	●	●	●	●
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	●	●	●●	●	●	●	●	●●
		PR.AC-2: Physical access to assets is managed and protected	●	●	●●●	●	●	●	●	●
		PR.AC-3: Remote access is managed	●	●	●	●	●	●	●	●
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	●	●	●●	●	●	●	●	●
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	●●	●	●●	●	●	●	●	●

	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	●●	●●	●●	●●	●●	●●●	●●●	●
		PR.AT-2: Privileged users understand roles & responsibilities	●	●	●	●	●	●●	●	●
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	●	●●	●	●	●●	●●	●●	●
		PR.AT-4: Senior executives understand roles & responsibilities	●●	●●	●●	●●	●	●●	●●	●
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	●●●	●●	●●●	●●●	●●●	●	●●	●
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	●	●	●	●	●	●	●	●●
		PR.DS-2: Data-in-transit is protected	●	●	●	●	●	●	●	●●
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	●	●	●	●	●	●	●	●●
		PR.DS-4: Adequate capacity to ensure availability is maintained	●	●	●	●	●	●	●	●
		PR.DS-5: Protections against data leaks are implemented	●	●	●	●	●	●	●	●●
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	●	●	●	●	●	●	●	●●●
		PR.DS-7: The development and testing environment(s) are separate from the production environment	●	●	●	●	●	●	●	●

	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	●	●	●●	●●	●	●●	●	●●
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	●	●	●	●	●	●	●●	●
		PR.IP-3: Configuration change control processes are in place	●	●	●	●	●	●	●	●
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	●	●	●●	●●	●	●●	●	●
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	●	●	●●	●●	●	●●	●●	●●
		PR.IP-6: Data is destroyed according to policy	●	●	●	●	●	●	●	●
		PR.IP-7: Protection processes are continuously improved	●	●	●●●	●	●	●	●	●
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	●	●	●	●	●	●	●	●
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	●	●	●	●●●	●	●●	●●●	●●●
		PR.IP-10: Response and recovery plans are tested	●	●	●●●	●●	●	●●	●●	●
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening)	●	●	●●●	●●	●	●●●	●●	●

		PR.IP-12: A vulnerability management plan is developed and implemented	●	●	●	●●	●	●●	●●	●●
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	●●	●●	●●●	●●●	●	●	●	●
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	●●	●●	●●	●●	●	●	●	●
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	●	●●	●●	●●	●●	●	●	●
		PR.PT-2: Removable media is protected and its use restricted according to policy	●	●	●	●	●	●	●	●
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	●	●	●●	●●	●●	●	●	●
		PR.PT-4: Communications and control networks are protected	●	●●●	●●●	●●●	●●●	●	●	●
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	●	●	●	●	●●	●●	●	●
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	●	●	●●	●	●●●	●●●	●	●
		DE.AE-3: Event data are aggregated and	●	●	●	●	●●	●	●	●

		correlated from multiple sources and sensors								
		DE.AE-4: Impact of events is determined	●	●●	●	●	●●	●●	●	●
		DE.AE-5: Incident alert thresholds are established	●	●●	●●	●	●●	●●	●	●
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	●●	●	●●	●	●	●	●	●
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	●●●	●	●●	●	●	●	●	●
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	●●	●	●●	●	●	●	●	●
		DE.CM-4: Malicious code is detected	●●	●	●●	●	●	●	●	●
		DE.CM-5: Unauthorized mobile code is detected	●	●	●	●	●	●	●	●
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	●	●	●●	●	●	●	●	●
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	●●	●	●●●	●	●	●	●	●
		DE.CM-8: Vulnerability scans are performed	●●●	●	●●	●	●	●	●	●●
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	●	●	●●	●●	●	●	●	●●
		DE.DP-2: Detection activities comply with all applicable requirements	●	●	●●●	●●●	●	●	●	●●
		DE.DP-3: Detection processes are tested	●	●	●●	●●	●	●	●	●●

		DE.DP-4: Event detection information is communicated to appropriate parties	●	●	●●	●●	●	●	●	●●
		DE.DP-5: Detection processes are continuously improved	●	●	●●	●●	●	●	●	●●
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	●●	●●	●	●●	●●	●	●	●
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	●●●	●	●●	●●	●	●	●	●
		RS.CO-2: Events are reported consistent with established criteria	●●	●	●●●	●●●	●	●●	●	●
		RS.CO-3: Information is shared consistent with response plans	●●	●	●●	●●	●	●●	●	●
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	●●●	●	●	●	●	●	●	●
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	●	●	●	●	●	●	●	●
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	●	●	●	●	●	●	●	●
		RS.AN-2: The impact of the incident is understood	●	●	●	●	●	●	●	●
		RS.AN-3: Forensics are performed	●	●	●	●	●	●	●	●
		RS.AN-4: Incidents are categorized consistent with response plans	●	●	●	●	●	●	●	●

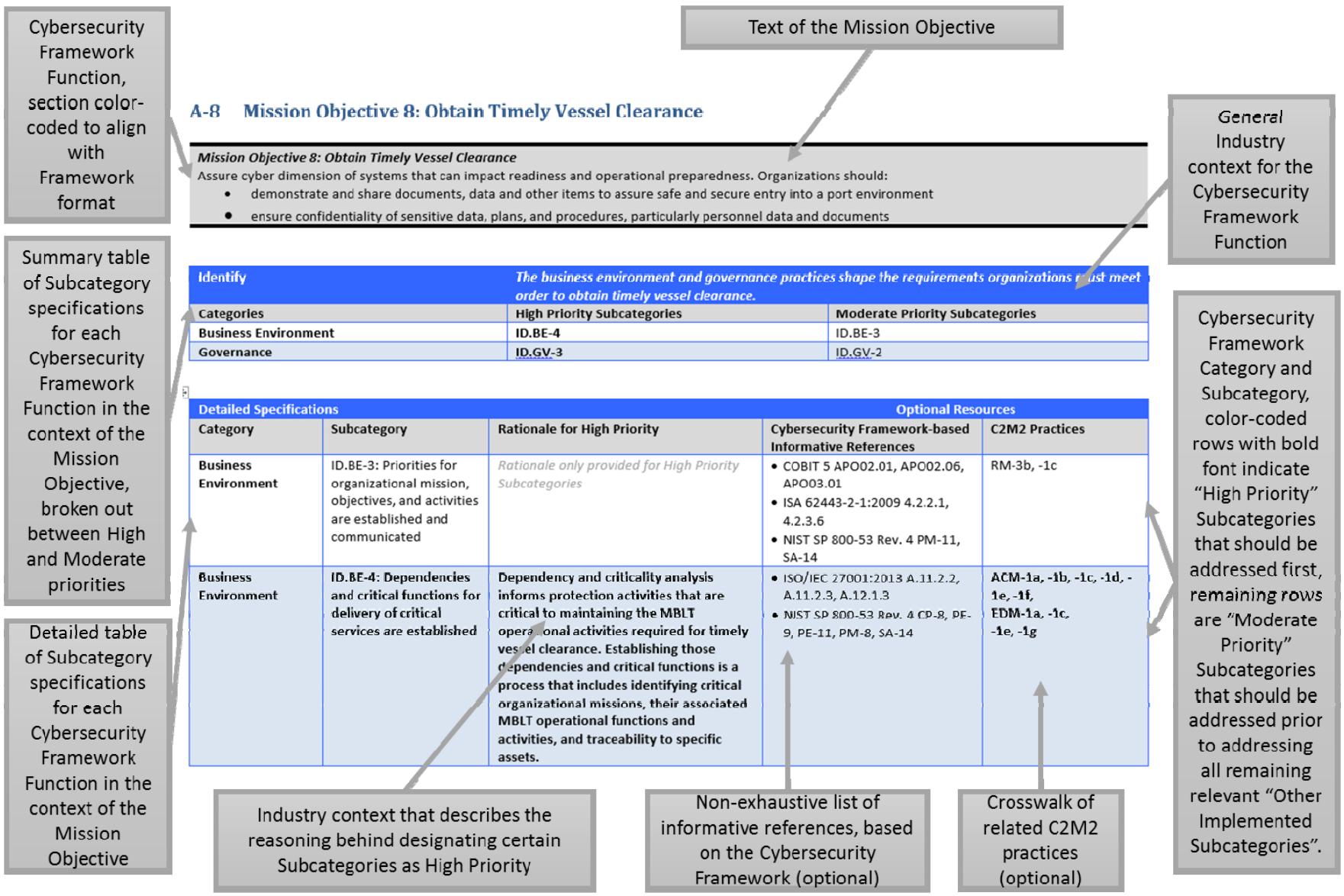
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	●	●	●	●	●	●●	●●	●
		RS.MI-2: Incidents are mitigated	●	●	●	●	●	●●	●●●	●
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	●	●	●	●	●	●●●	●●	●
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	●	●	●	●	●	●	●●●	●
		RS.IM-2: Response strategies are updated	●	●	●	●	●	●	●●	●
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	●●	●●	●●	●●	●	●	●	●
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	●	●	●	●●	●	●	●	●
		RC.IM-2: Recovery strategies are updated	●	●	●	●●	●	●	●	●

	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	●	●	●	●	●	●	●	●
		RC.CO-2: Reputation after an event is repaired	●	●	●	●	●	●	●	●
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	●	●	●	●	●	●	●	●●

Appendix A – Detailed Subcategory Specifications

This MBLT CFP defines the desired minimum state of cybersecurity by identifying the minimum set of Cybersecurity Framework Categories and Subcategories for each of the eight Mission Objectives required to conduct MBLT operations in a more secure manner. Appendix A is divided into a subsection for each of the eight Mission Objectives listed in Section 6.1, Table 6-1. Each Mission Objective subsection in Appendix A includes both a summary and detailed table of High and Moderate Priority Subcategory specifications in the Profile by Cybersecurity Framework Function and Category. Figure A-1 provides a legend that describes the layout of the detailed Profile content provided.

Figure A-1. Appendix A Content Legend


Cybersecurity Framework Function, section color-coded to align with Framework format
Text of the Mission Objective
A-8 Mission Objective 8: Obtain Timely Vessel Clearance
Mission Objective 8: Obtain Timely Vessel Clearance
Assure cyber dimension of systems that can impact readiness and operational preparedness. Organizations should:
demonstrate and share documents, data and other items to assure safe and secure entry into a port environment
ensure confidentiality of sensitive data, plans, and procedures, particularly personnel data and documents
General Industry context for the Cybersecurity Framework Function
Summary table of Subcategory specifications for each Cybersecurity Framework Function in the context of the Mission Objective, broken out between High and Moderate priorities
Identify
The business environment and governance practices shape the requirements organizations must meet order to obtain timely vessel clearance.
Categories
High Priority Subcategories
Moderate Priority Subcategories
Business Environment
ID.BE-4
ID.BE-3
Governance
ID.GV-3
ID.GV-2
Detailed Specifications
Optional Resources
Category
Subcategory
Rationale for High Priority
Cybersecurity Framework-based Informative References
C2M2 Practices
Business Environment
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
Rationale only provided for High Priority Subcategories
COBIT 5 APO02.01, APO02.06, APO03.01
ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6
NIST SP 800-53 Rev. 4 PM-11, SA-14
RM-3b, -1c
Business Environment
ID.BE-4: Dependencies and critical functions for delivery of critical services are established
Dependency and criticality analysis informs protection activities that are critical to maintaining the MBLT operational activities required for timely vessel clearance. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated MBLT operational functions and activities, and traceability to specific assets.
ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3
NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14
ACM-1a, -1b, -1c, -1d, -1e, -1f, EDM-1a, -1c, -1e, -1g
Cybersecurity Framework Category and Subcategory, color-coded rows with bold font indicate "High Priority" Subcategories that should be addressed first, remaining rows are "Moderate Priority" Subcategories that should be addressed prior to addressing all remaining relevant "Other Implemented Subcategories".
Detailed table of Subcategory specifications for each Cybersecurity Framework Function in the context of the Mission Objective
Industry context that describes the reasoning behind designating certain Subcategories as High Priority
Non-exhaustive list of informative references, based on the Cybersecurity Framework (optional)
Crosswalk of related C2M2 practices (optional)

A-1 Mission Objective 1: Maintain Personnel Safety

Mission Objective 1: Maintain Personnel Safety

Cybersecurity-effect on process control systems impacts personnel safety. Organizations should:

- manage risks to the organization and industry using a structured process
- identify and train personnel on interdependence of cybersecurity with operational responsibilities
- implement Detect/Respond/Remediate activities where cybersecurity adversely affects personnel safety

Identify	**Risk Assessments and risk management processes are the primary method used to identify procedures, technologies, and equipment that may impact an organization's ability to maintain personnel safety.**	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Risk Assessment	**ID.RA-1**, **ID.RA-5**, **ID.RA-6**	ID.RA-2, ID.RA-3, ID.RA-4
Risk Management Strategy	**ID.RM-1**	ID.RM-2, ID.RM-3

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	**ID.RA-1: Asset vulnerabilities are identified and documented**	**Cybersecurity vulnerabilities in MBLT operations that are exploited can lead to unpredictable behaviors of control systems, including malfunctions that cause personnel safety issues ranging from minor harms to death. Identifying vulnerabilities for control systems assets, and understanding how those vulnerabilities may impact personnel safety, is the starting point for conducting realistic risk assessments and determining appropriate risk responses.**	• **CCS CSC 4** • **COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04** • **ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12** • **ISO/IEC 27001:2013 A.12.6.1, A.18.2.3** • **NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5**	**SA-1a, IR-1C, IAM-2a, -2b, -2c, 2d, -2e, -2f, -2g, -2h**
Risk Assessment	ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.6.1.4 • NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5	TVM-1a, -1b, -2a, -2b
Risk Assessment	ID.RA-3: Threats, both internal and external, are identified and documented	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	TVM-1a, -1b, -1d, -1e, -1j, RM-2j

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	ID.RA-4: Potential business impacts and likelihoods are identified	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14	TVM-1d, -1f, -1c, 1i
Risk Assessment	**ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk**	**Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in an organization's operating environment for MBLT operations, as well as how the unique combination(s) of them affect the organization's risk posture, is necessary for conducting thorough and accurate risk assessments. Examining threats and vulnerabilities in the context of the organization's particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect personnel safety, and also provides input into monitoring plans.**	• **COBIT 5 APO12.02** • **ISO/IEC 27001:2013 A.12.6.1** • **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**	**RM-1c, -2j, TVM-2m**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	**ID.RA-6: Risk responses are identified and prioritized**	**In order to protect personnel safety during maritime bulk liquid transport operations, risks that impact personnel safety must be identified as such, and those personnel safety implications must be considered in the prioritization given to risks in the organization's risk response strategies. There are five basic types of responses to risk with some overlap in between: (i) accept; (ii) avoid; (iii) mitigate; (iv) share; and (v) transfer.[22] For risks that impact personnel safety, "accept" may only be an appropriate option under limited circumstances.[23]**	• **COBIT 5 APO12.05, APO13.02** • **NIST SP 800-53 Rev. 4 PM-4, PM-9** • **NIST SP 800-39**	**RM-2e, 1c, -2j, TVM-1d, IR-3m**

[22] NIST SP 800-39, *Managing Information Security Risk, Organization, Mission, and Information System View*, March 2011. Appendix H, "Risk Response Strategies"

[23] NIST has conducted extensive research regarding risk management practices. FIPS 199, while merely informative for the purposes of these Mission Objectives, defines levels of risk in terms of low, moderate, and high that may provide useful delineations in some contexts.

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Management Strategy	**ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders**	**Addressing personnel safety risks during MBLT operations in accordance with risk management strategies requires clearly defined procedures and engaged stakeholders that understand their roles in executing risk management activities. Documenting activities and roles allows all stakeholders to: (i) come to a common understanding of the risks and risk management processes, (i) collaboratively determine the most effective ways to integrate risk management processes into the operational environment, and (iii) understand the responsibilities for which they are held accountable.**	• **COBIT 5 APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02** • **ISA 62443-2-1:2009 4.3.4.2** • **NIST SP 800-53 Rev. 4 PM-9**	**RM-2a, -2b, -1a, -1b, -2c, -2d, -2e, 2g, -3a, -3b, -3c, -3d, -1c, -1d, -1e, -2h, -2j,-3g, -3h, -3i**
Risk Management Strategy	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.2.6.5 • NIST SP 800-53 Rev. 4 PM-9	RM-1c, -1e
Risk Management Strategy	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	*Rationale only provided for High Priority Subcategories*	• NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14	RM-1b, -1c

Protect	***Access Control, Awareness and Training, and Maintenance were identified as the priority activities. Without access control knowledge of personnel's location is inhibited. Without awareness and training personnel are not prepared to manage a personnel security incident. Without maintenance, systems will not be ready to deal with personnel safety issues.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Access Control	N/A	PR.AC-5
Awareness and Training	**PR.AT-5**	PR.AT-1, PR.AT-4
Maintenance	N/A	PR.MA-1, PR.MA-2

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Access Control	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, SC-7	CPM-3a, -3b, -3b, -3d
Awareness and Training	PR.AT-1: All users are informed and trained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13	WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-4: Senior executives understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
Awareness and Training	**PR.AT-5: Physical and information security personnel understand roles & responsibilities**	**Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in personnel safety issues in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, personnel must have an understanding of how to prioritize responsibilities as needed.**	• **CCS CSC 9** • **COBIT 5 APO07.03** • **ISA 62443-2-1:2009 4.3.2.4.2** • **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** • **NIST SP 800-53 Rev. 4 AT-3, PM-13**	**WM-1a, -1b, -1c, -1d, -1e, -1f, -1g**
Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.3.3.7 • ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 • NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5	ACM-3b, -4c, -3f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4	SA-1a, IR-1C, IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h

Detect	***Real time awareness of monitoring systems, alerts is critical to personnel safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Security Continuous Monitoring	**DE.CM-2**, **DE.CM-8**	DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-7

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	*Rationale only provided for High Priority Subcategories*	• CCS CSC 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	SA-2a, -2b, -2e, -2f, -2g, -2i, TVM-1d
Security Continuous Monitoring	**DE.CM-2: The physical environment is monitored to detect potential cybersecurity events**	**Monitoring facilities and physical equipment, devices, systems, and other assets for access issues and other activities is one of the primary ways anomalies can lead to cybersecurity events that impact personnel safety are identified.**	• **ISA 62443-2-1:2009 4.3.3.3.8** • **NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20**	**SA-2a, -2b, -2e, -2i**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Security Continuous Monitoring	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	*Rationale only provided for High Priority Subcategories*	• ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	SA-2a, -2b, -2e, -2i
Security Continuous Monitoring	DE.CM-4: Malicious code is detected	*Rationale only provided for High Priority Subcategories*	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3	SA-2a, -2b, -2e, -2i, CPM-4a
Security Continuous Monitoring	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	*Rationale only provided for High Priority Subcategories*	• NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	SA-2a, -2b, -2e, -2f, -2g, -2i, TVM-1d
Security Continuous Monitoring	**DE.CM-8: Vulnerability scans are performed**	**Vulnerability scanning proactively identifies weaknesses in IT or OT systems, system security procedures, internal controls, or other activities that could be exploited by a threat source to cause a cybersecurity event during MBLT operations, including cybersecurity events that impact personnel safety.**	• **COBIT 5 BAI03.10** • **ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7** • **ISO/IEC 27001:2013 A.12.6.1** • **NIST SP 800-53 Rev. 4 RA-5**	**TVM-2e, -2i, -2j, -2k, RM-1c**

Respond	***Proper response and communication plan development and utilization is critical in the response phase of maintaining personnel safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Response Planning	N/A	RS.RP-1
Communications	**RS.CO-1, RS.CO-4**	RS.CO-2, RS.CO-3

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Response Planning	RS.RP-1: Response plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR8	IR-3d
Communications	**RS.CO-1: Personnel know their roles and order of operations when a response is needed**	**Effective and efficient response to a cybersecurity event requires that all IT and OT personnel know and understand their role prior to response activities commencing. For cybersecurity events that may impact personnel safety, timing can be critical. Failure to properly execute response procedures quickly, adequately, and in the correct order can result in issues ranging from minor harms to death.**	• **ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4** • **ISO/IEC 27001:2013 A.6.1.1, A.16.1.1** • **NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8**	**IR-3a, -5b**
Communications	RS.CO-2: Events are reported consistent with established criteria	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	IR-1a, IR-1b

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Communications	RS.CO-3: Information is shared consistent with response plans	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4	ISC-1a, -1b,-1c, -1d, IR-3d, -3i, 3l
Communications	**RS.CO-4: Coordination with stakeholders occurs consistent with response plans**	**Responding to a cybersecurity event takes coordination across multiple parts of the business to ensure the right activities can be conducted at the right time. Response plans describe the minimum activities that must be coordinated between stakeholders for a successful response to a cybersecurity event.**	• **ISA 62443-2-1:2009 4.3.4.5.5** • **NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8**	**IR-3d, -5b**

Recover	***Recovery plan development and utilization are critical to the recover phase of maintaining personnel safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Recovery Planning	N/A	RC.RP-1

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	IR-3b, -3d, -3o, -4k

A-2 Mission Objective 2: Maintain Environmental Safety

Mission Objective 2: Maintain Environmental Safety

Cybersecurity-effect on process control systems impacts environmental safety. Organizations should:

- manage risks to the organization and industry using a structured process
- identify and train personnel on interdependence of cybersecurity with operational responsibilities
- manage prominent and increasing role of automated systems in maintaining quality control of product during safe transport
- implement Detect/Respond/Remediate activities where cybersecurity adversely affects environmental safety

Identify	***Asset management and risk assessment were seen as the most significant Categories in the Identify functional area of the Cybersecurity Framework.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Asset Management	**ID.AM-1**, **ID.AM-5**	ID.AM-2
Risk Assessment	N/A	ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Asset Management	**ID.AM-1: Physical devices and systems within the organization are inventoried**	**Maintaining a current inventory of the physical devices and systems that support MBLT operations provides the foundation for identifying and prioritizing assets that have environmental safety impacts.**	• **CCS CSC 1** • **COBIT 5 BAI09.01, BAI09.02** • **ISA 62443-2-1:2009 4.2.3.4** • **ISA 62443-3-3:2013 SR 7.8** • **ISO/IEC 27001:2013 A.8.1.1, A.8.1.2** • **NIST SP 800-53 Rev. 4 CM-8**	**ACM-1a, -1c, -1e, -1f**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Asset Management	ID.AM-2: Software platforms and applications within the organization are inventoried	*Rationale only provided for High Priority Subcategories*	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8	ACM-1a, -1c, -1e, -1f
Asset Management	**ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value**	**Potential environmental safety impacts of MBLT operations resources are necessary factors to consider when prioritizing resources. Resource prioritization informs how Cybersecurity Framework functions are performed with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.**	• **COBIT 5 APO03.03, APO03.04, BAI09.02** • **ISA 62443-2-1:2009 4.2.3.6** • **ISO/IEC 27001:2013 A.8.2.1** • **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14**	**ACM-1a, -1b, -1c, -1d**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	*Rationale only provided for High Priority Subcategories*	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	TVM-2a, -2b, -2d, -2e, -2f, -2i, -2j, -2k, -2l, -2m
Risk Assessment	ID.RA-3: Threats, both internal and external, are identified and documented	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16	TVM-1a, -1b, -1d, -1e, 1j, RM-2j
Risk Assessment	ID.RA-4: Potential business impacts and likelihoods are identified	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14	TVM-1d, -1f, -1c, 1i
Risk Assessment	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.02 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16	RM-1c, -2j, TVM-2m

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	ID.RA-6: Risk responses are identified and prioritized	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.05, APO13.02 • NIST SP 800-53 Rev. 4 PM-4, PM-9	RM-2e, 1c, -2j, TVM-1d, IR-3m

Protect	***Training, good maintenance programs and proper deployment of protective technology are critical to maintaining environmental safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Awareness and Training	N/A	PR.AT-1, PR.AT-3, PR.AT-4, PR.AT-5
Maintenance	N/A	PR.MA-1, PR.MA-2
Protective Technology	**PR.PT-4**	PR.PT-1

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-1: All users are informed and trained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13	WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
Awareness and Training	PR.AT-4: Senior executives understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
Awareness and Training	PR.AT-5: Physical and information security personnel understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Maintenance	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4.3.3.3.7 • ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5 • NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5	ACM-3b, -4c, -3f
Maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4	SA-1a, IR-1c, IAM-2a, -2b, -2c, -2d,-2e, -2f, -2g, -2h
Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	*Rationale only provided for High Priority Subcategories*	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family	SA-1a, -2a, -1b, -1c, -2e, -4a, -1d, -1e, -3d, -4e, -4f, -4g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	**PR.PT-4: Communications and control networks are protected**	**Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing useful operational and management capabilities, and can also be a source of great vulnerability if not well protected. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in environmental safety issues.**	• **CCS CSC 7** • **COBIT 5 DSS05.02, APO13.01** • **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** • **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** • **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7**	**CPM-3a, -3b, -3c, -3d**

Detect	***Early detection of anomalies and events is critical to maintaining environmental safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Anomalies and Events	N/A	DE.AE-4, DE.AE-5

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Anomalies and Events	DE.AE-4: Impact of events is determined	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI 4	IR-2b, -2d, -2g, TVM-1d, RM-2j
Anomalies and Events	DE.AE-5: Incident alert thresholds are established	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	IR-2a, -2d, 2g ,-2j, TVM-1d, SA-1d, RM-2j

Respond	***Proper response and communication plan development and utilization is critical in the response phase of maintaining envrionmental safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Response Planning	N/A	RS.RP-1

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Response Planning	RS.RP-1: Response plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR8	**IR-3d**

Recover	***Proper recovery planning is critical to mitigations when maintaining environmental safety***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Recovery Planning	N/A	RC.RP-1

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	IR-3b, -3d, -3o, -4k

A-3 Mission Objective 3: Maintain Operational Security

Mission Objective 3: Maintain Operational Security

Cybersecurity-effect on security control systems impacts operational safety and security. Organizations should:

- manage risks to the organization and industry using a structured process
- identify and train personnel on interdependence of cybersecurity with operational responsibilities
- manage prominent and increasing role of automated systems in maintaining physical control of infrastructure
- implement Detect/Respond/Remediate activities where cybersecurity adversely affects safety and security

Identify	***Proper risk assessment is critical to maintaining operational security***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Risk Assessment	**ID.RA-5**	ID.RA-1

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	*Rationale only provided for High Priority Subcategories*	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	TVM-2a, -2b, -2d, -2e, -2f, -2i, -2j, -2k, -2l, -2m, RM-1c, -2j

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	**ID.RA-5: Threats, vulnerabilities, likelihood, and impacts are used to determine risk**	**Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in an organization's operating environment for MBLT operations as well as how the unique combination(s) of them affect the organization's risk posture is necessary for conducting thorough and accurate risk assessments. Examining threats and vulnerabilities in the context of the organization's particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect operational security, and also provides input into monitoring plans.**	• **COBIT 5 APO12.02** • **ISO/IEC 27001:2013 A.12.6.1** • **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**	**RM-1c,-2j, TVM-2m**

Protect	Proper risk assessment is critical to maintaining operational security	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Access Control	**PR.AC-2**	PR.AC-1, PR.AC-4, PR.AC-5
Awareness and Training	**PR.AT-5**	PR.AT-1, PR.AT-4
Information Protection Processes & Procedures	**PR.IP-7**, **PR.IP-10**, **PR.IP-11**	PR.IP-1, PR.IP-4, PR.IP-5
Maintenance	**PR.MA-1**	PR.MA-2
Protective Technology	**PR.PT-4**	PR.PT-1, PR.PT-3

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users	*Rationale only provided for High Priority Subcategories*	• CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family	IAM-1a, -1b, -1c, -1d, -1e, -1f, -1g, RM-1c
Access Control	**PR.AC-2: Physical access to assets is managed and protected**	**Physical access to MBLT operations assets may allow manipulation of those assets in a way that disrupts operations, including disabling an asset and halting operations. Operational harms may range from minor inconvenience to operations to large-scale industry-wide impacts, and may lead to issues that span other Mission Objectives, such as Maintaining Personnel Safety and Maintaining Environmental Safety.**	• **COBIT 5 DSS01.04, DSS05.05** • **ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8** • **ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3** • **NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE5, PE-6, PE-9**	**IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g**
Access Control	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	*Rationale only provided for High Priority Subcategories*	• CCS CSC 12, 15 • ISA 62443-2-1:2009 4.3.3.7.3 • ISA 62443-3-3:2013 SR 2.1 • ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 • NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16	IAM-2d

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Access Control	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.3.4 • ISA 62443-3-3:2013 SR 3.1, SR 3.8 • ISO/IEC 27001:2013 A.13.1.1, A.13.1.3, A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, SC-7	CPM-3a, -3b, -3c, -3d
Awareness and Training	PR.AT-1: All users are informed and trained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13	WM-3a, -3b, -3c, -3d, -3g, -3h, -4a
Awareness and Training	PR.AT-4: Senior executives understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	**PR.AT-5: Physical and information security personnel understand roles & responsibilities**	**Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in operational security issues in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, personnel must have an understanding of how to prioritize responsibilities as needed.**	• **CCS CSC 9** • **COBIT 5 APO07.03** • **ISA 62443-2-1:2009 4.3.2.4.2** • **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** • **NIST SP 800-53 Rev. 4 AT-3, PM-13**	**WM-1a, -1b, -1c, -1d, -1e, -1f, -1g**
Information Protection Processes & Procedures	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	ACM-2a, -2b, -2c, -2d, -2e

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	IR-4a, -4b
Information Protection Processes & Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	ACM-4f, RM-3f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	**PR.IP-7: Protection processes are continuously improved**	**Regularly examining the effectiveness and efficiency of protection processes provides organizations with valuable feedback regarding how their cybersecurity efforts to protect MBLT operations assets are performing, and where improvements need to be made over time as problems or improved practices are identified. Additionally, the threat environment for MBLT operations may continue to evolve even when organizations do not make signification changes to IT and OT assets (e.g., new vulnerabilities for an existing technology may be discovered).**	• **COBIT 5 APO11.06, DSS04.05** • **ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8** • **NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6**	**CPM-1g**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	**PR.IP-10: Response and recovery plans are tested**	**Periodically testing response and recovery plans for MBLT operations helps organizations determine the effectiveness of the plans and identify any necessary improvements as the environment changes over time. Testing response and recovery plans prior to invoking them during a real cybersecurity event provides stakeholders experience executing the plans in a collaborative learning environment so that they are more practiced when implementing the plans during real-time response and recovery efforts, increasing the organization's chances of more effectively restoring operational security efficiently and effectively.**	• **ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11** • **ISA 62443-3-3:2013 SR 3.3** • **ISO/IEC 27001:2013 A.17.1.3** • **NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14**	**IR-3e, -4f, -3k, -4i, -4j**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	**PR.IP-11: Cybersecurity is included in human resource practices (e.g. de-provisioning, personnel screening)**	**MBLT operations rely on personnel to operate and maintain IT and OT assets. Including cybersecurity in human resources practices helps ensure that the right people have access to the right access at the right times through activities, such as: screening personnel against applicable safety and knowledge conditions, provisioning and de-provisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their operational security-related roles and responsibilities. Including cybersecurity in human resource practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with operational security-related policies and procedures.**	• **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** • **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** • **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4** • **NIST SP 800-53 Rev. 4 PS Family**	**WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Maintenance	**PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools**	**Properly maintaining MBLT assets safeguards against preventable issues that could impact operational safety. Managing maintenance through a defined approval process and with controlled tools protects the organization from introducing unnecessary risks, such as performing maintenance during a time that impacts other assets, changing implemented controls in a way that renders them ineffective, running tools that have not been scanned for malicious activity, or allowing access to unescorted and/or unauthorized individuals.**	• **COBIT 5 BAI09.03** • **ISA 62443-2-1:2009 4.3.3.3.7** • **ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5** • **NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5**	**ACM-3b, -4c, -3f**
Maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4	SA-1a, IR-1c, IAM-2a, -2b, -2c, -2d, -2f, -2g, -2h

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	*Rationale only provided for High Priority Subcategories*	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family	SA-1a, -2a, 1b, -1c, -2e, -4a, -1d, -1e, -3d, -4e, -4f, -4g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7	IAM-2a, -2b, 2c, -2d, -2e, -2f, -2g, -2h, -2i

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	**PR.PT-4: Communications and control networks are protected**	**Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing useful operational and management capabilities, and can also be a source of great vulnerability if not well protected. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in operational security issues.**	• **CCS CSC 7** • **COBIT 5 DSS05.02, APO13.01** • **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** • **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** • **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7**	**CPM-3a, -3b, -3c, -3d**

Detect	***Having robust detection processes which continuously monitor sensors and alarms for anomalies and events are critical to maintaining operational safety.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Anomalies and Events	**DE.AE-1**	DE.AE-2, DE.AE-5
Security Continuous Monitoring	**DE.CM-7**	DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-6, DE.CM-8
Detection Processes	**DE.DP-2**	DE.DP-1, DE.DP-2, DE-DP-3, DE.DP-4, DE.DP-5

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Anomalies and Events	**DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed**	**Understanding the baseline of network operations and expected data flows during typical MBLT operations supports operational security by providing a means of comparing current activities against expectations in order to identify anomalies or other events that may require analysis and response.**	• **COBIT 5 DSS03.01** • **ISA 62443-2-1:2009 4.4.3.3** • **NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4**	**SA-2a**
Anomalies and Events	DE.AE-2: Detected events are analyzed to understand attack targets and methods	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • ISO/IEC 27001:2013 A.16.1.1, A.16.1.4 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI4	IR-1f, -2l, 3h
Anomalies and Events	DE.AE-5: Incident alert thresholds are established	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	IR-2a, -2d, -2g, TVM-1d, SA-2d, RM-2j
Security Continuous Monitoring	DE.CM-1: The network is monitored to detect potential cybersecurity events	*Rationale only provided for High Priority Subcategories*	• CCS CSC 14, 16 • COBIT 5 DSS05.07 • ISA 62443-3-3:2013 SR 6.2 • NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	SA-2a, -2 b, 2e, -2f, -2g, -2i, TVM-1d

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Security Continuous Monitoring	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.3.3.8 • NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE20	SA-2a, -2b, -2e, -2i
Security Continuous Monitoring	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	*Rationale only provided for High Priority Subcategories*	• ISA 62443-3-3:2013 SR 6.2 • ISO/IEC 27001:2013 A.12.4.1 • NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	SA-2a, -2b, 2e, 2i
Security Continuous Monitoring	DE.CM-4: Malicious code is detected	*Rationale only provided for High Priority Subcategories*	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.3.4.3.8 • ISA 62443-3-3:2013 SR 3.2 • ISO/IEC 27001:2013 A.12.2.1 • NIST SP 800-53 Rev. 4 SI-3	SA-2a, -2b, -2e, -2i, CPM-4a
Security Continuous Monitoring	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA9, SI-4	EDM-2a, -2j, -2n, SA-2a, -2b, -2e

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Security Continuous Monitoring	**DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed**	**Monitoring for unauthorized activities supports operational security by identifying events, in accordance with defined monitoring objectives, that may signify a cybersecurity issue, and providing the necessary information to support an appropriate risk response. Outputs from monitoring MBLT operations provide input into event correlation and analysis tools, alert mechanisms, and the response process.**	• **NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4**	**SA-2a, -2b, -2e, -2f, -2g, -2i, TVM-1d**
Security Continuous Monitoring	DE.CM-8: Vulnerability scans are performed	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI03.10 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 RA-5	TVM-2e, -2i, -2j, -2k, RM-1c
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	*Rationale only provided for High Priority Subcategories*	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	WM-1a, -1d, -1f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Detection Processes	**DE.DP-2: Detection activities comply with all applicable requirements**	**Monitoring and other detection activities that support operational security must be conducted in accordance with federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies that apply to MBLT operations. Failing to comply with applicable requirements may result in issues such as gaps in detection activities, challenges pursuing sanctions, or legal action when warranted.**	• **ISA 62443-2-1:2009 4.4.3.2** • **ISO/IEC 27001:2013 A.18.1.4** • **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4**	**IR-1d, -5a, -1g, -5f, TVM-1d, RM-1c, -2j**
Detection Processes	DE.DP-3: Detection processes are tested	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	IR-3e, -3j
Detection Processes	DE.DP-4: Event detection information is communicated to appropriate parties	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	IR-1b, -3c, -3n, ISC-1a, -1c, -1d, -1h, -1j
Detection Processes	DE.DP-5: Detection processes are continuously improved	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	IR-3h, -3k

Respond	*Proper communications channels and procedures are key to response to an operational security incident*	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Communications	**RS.CO-2**	RS.CO-1RS.CO-3

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	IR-3a, -5b
Communications	**RS.CO-2: Events are reported consistent with established criteria**	**Reporting MBLT operations events that have been identified as cybersecurity-relevant maintains operational security by ensuring the necessary information is reported to the correct entities in a timely manner so that a proper response can be initiated.**	• **ISA 62443-2-1:2009 4.3.4.5.5** • **ISO/IEC 27001:2013 A.6.1.3, A.16.1.2** • **NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8**	**IR-1a, -1b**
Communications	RS.CO-3: Information is shared consistent with response plans	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4	ISC-1a, -1b, -1c, -1d, IR-3d, -3i, -3l

Recover	***Proper recovery planning is critical to maintaining operational security***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Recovery Planning	N/A	RC.RP-1

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	IR-3b, -3d, -3o, -4k

A-4 Mission Objective 4: Maintain Preparedness

Mission Objective 4: Maintain Preparedness

Cybersecurity-effect on systems readiness that can impact operations including maintenance, documentation and testing for safety and security. Organizations should:

- develop systems and train personnel to integrate cybersecurity-impacts on resilience in maintaining mission assurance
- implement resilience-aware activities including
    - risk mitigation procedures
    - ongoing situational awareness
    - backup/resilience/fail-safe modes
    - regular preventive maintenance

Identify	***Risk assessment is key to proper identification of risks in the maintain preparedness Mission Objective***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Risk Assessment	**ID.RA-5**	ID.RA-1

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	*Rationale only provided for High Priority Subcategories*	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	TVM-1a, -1b, -2a, -2b, -2d

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	**ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk**	**Understanding the threats and vulnerabilities related to the specific IT and OT technologies employed in an organization's operating environment for MBLT operations as well as how the unique combination(s) of them affect the organization's risk posture is necessary for conducting thorough and accurate risk assessments. Examining threats and vulnerabilities in the context of the organization's particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect the organization's ability to maintain preparedness and also provides input into monitoring plans.**	• **COBIT 5 APO12.02** • **ISO/IEC 27001:2013 A.12.6.1** • **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**	**RM-1c, -2j, TVM-2m**

Protect	*Proper training, planning & processes, maintenance and communications are key to maintaining preparedness*	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Awareness and Training	**PR.AT-5**	PR.AT-1, PR.AT-4
Information Protection Processes & Procedures	**PR.IP-9**	PR.IP-1, PR.IP-4, PR.IP-5, PR.IP-10, PR.IP-11, PR.IP-12
Maintenance	**PR.MA-1**	PR.MA-2
Protective Technology	**PR.PT-4**	PR.PT-1, PR.PT-3

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-1: All users are informed and trained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13	WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i
Awareness and Training	PR.AT-4: Senior executives understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, i1c, -1d, -1e, -1f, -1g
Awareness and Training	**PR.AT-5: Physical and information security personnel understand roles & responsibilities**	**Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in issues with maintaining preparedness in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, personnel must have an understanding of how to prioritize responsibilities as needed.**	• **CCS CSC 9** • **COBIT 5 APO07.03** • **ISA 62443-2-1:2009 4.3.2.4.2** • **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** • **NIST SP 800-53 Rev. 4 AT-3, PM-13**	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes and Procedures	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	ACM-2a, -2b, -2c, -2d, -2e
Information Protection Processes and Procedures	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	IR-4a, -4b

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes and Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	ACM-4f, RM-3f
Information Protection Processes and Procedures	**PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed**	**MBLT operations response and recovery plans define the degree of IT and OT operations necessary to return to a desired minimum state of operations after a cybersecurity event. Developing and managing these plans in coordination with incident response processes ensures that the necessary activities occur when a cybersecurity event is identified. Instituting processes to manage response and recovery plans ensures they are periodically updated, allowing the organization to maintain an acceptable level of preparedness.**	• **COBIT 5 DSS04.03** • **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1** • **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2** • **NIST SP 800-53 Rev. 4 CP-2, IR-8**	**IR-4c, -3f, -4d. -4f, -5a, -5b, -5d, -3k, -3m, -4j, -5e, -5f, -5g, -5h, -5i, TVM-1d, RM-1c**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes and Procedures	PR.IP-10: Response and recovery plans are tested	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	IR-3e, -3k, -4f, -4i, -4j
Information Protection Processes and Procedures	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS Family	WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h
Information Protection Processes and Procedures	PR.IP-12: A vulnerability management plan is developed and implemented	*Rationale only provided for High Priority Subcategories*	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	TVM-3a, -3e

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Maintenance	**PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools**	**Properly maintaining MBLT assets safeguards against preventable issues that could impact the organization's ability to maintain an acceptable level of preparedness. Managing maintenance through a defined approval process and with controlled tools protects the organization from introducing unnecessary risks, such as performing maintenance during a time that impacts other assets, changing implemented controls in a way that renders them ineffective, running tools that have not been scanned for malicious software, or allowing access to unescorted and/or unauthorized individuals.**	• **COBIT 5 BAI09.03** • **ISA 62443-2-1:2009 4.3.3.3.7** • **ISO/IEC 27001:2013 A.11.1.2, A.11.2.4, A.11.2.5** • **NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5**	**ACM-3b, -4c, -3f**
Maintenance	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.04 • ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8 • ISO/IEC 27001:2013 A.11.2.4, A.15.1.1, A.15.2.1 • NIST SP 800-53 Rev. 4 MA-4	SA-1a, IR-1c, IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	*Rationale only provided for High Priority Subcategories*	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family	SA-1a, -1b, -1c, -1d, -1e, -2a, -2e, -3d, -4a, -4f, -4g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7	IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h, -2i

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	**PR.PT-4: Communications and control networks are protected**	**Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing useful operational and management capabilities, and can also be a source of great vulnerability if not well protected. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in preparedness issues.**	• **CCS CSC 7** • **COBIT 5 DSS05.02, APO13.01** • **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** • **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** • **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7**	**CPM-3a, -3b, -3c, -3d**

Detect	***Detection processes must comply with applicable rules and regulations***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Detection Processes	**DE.DP-2**	DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	*Rationale only provided for High Priority Subcategories*	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	WM-1a, -1d, -1f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Detection Processes	**DE.DP-2: Detection activities comply with all applicable requirements**	**Monitoring and other detection activities that support the ability to maintain an acceptable level of preparedness must be conducted in accordance with federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies, that apply to MBLT operations. Failing to comply with applicable requirements may result in issues such as gaps in detection activities, challenges pursuing sanctions, or legal action when warranted.**	• **ISA 62443-2-1:2009 4.4.3.2** • **ISO/IEC 27001:2013 A.18.1.4** • **NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4**	**IR-1d, 5a, -1g, -5f, TVM-1d, RM-1c, RM-2j**
Detection Processes	DE.DP-3: Detection processes are tested	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	IR-3e, -3j
Detection Processes	DE.DP-4: Event detection information is communicated to appropriate parties	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	IR-1b, -3c, -3n, ISC-1a, -1c, -1d, -1h, -1j

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Detection Processes	DE.DP-5: Detection processes are continuously improved	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	IR-3h, -3k

Respond	***Response plans that are property designed, built to, approved, inspected and trained for are key to maintaining preparedness.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Response Planning	N/A	RS.RP-1
Communications	**RS.CO-2**	RS.CO-1, RS.CO-3

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Response Planning	RS.RP-1: Response plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR8	IR-3d
Communications	RS.CO-1: Personnel know their roles and order of operations when a response is needed	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8	IR-3d

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Communications	**RS.CO-2: Events are reported consistent with established criteria**	**Reporting MBLT operations events that have been identified as cybersecurity-relevant helps organizations maintain an acceptable level of preparedness by ensuring the necessary information is reported to the correct entities in a timely manner so that a proper response can be initiated.**	• **ISA 62443-2-1:2009 4.3.4.5.5** • **ISO/IEC 27001:2013 A.6.1.3, A.16.1.2** • **NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8**	**IR-3d**
Communications	RS.CO-3: Information is shared consistent with response plans	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4	IR-3d

Recover	***Recovery planning and adapting capabilities based on field experience are key to maintaining preparedness.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Recovery Planning	N/A	RC.RP-1
Improvements	N/A	RC.IM-1, RC.IM-2

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Recovery Planning	RC.RP-1: Recovery plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• CCS CSC 8 • COBIT 5 DSS02.05, DSS03.04 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8	IR-3b, -3d, -3o, -4k

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Improvements	RC.IM-1: Recovery plans incorporate lessons learned	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI05.07 • ISA 62443-2-1:2009 4.4.3.4 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	IR-3h, -4i, -3k
Improvements	RC.IM-2: Recovery strategies are updated	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI07.08 • NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	IR-3h, -3k

A-5 Mission Objective 5: Maintain Quality of Product

Mission Objective 5: Maintain Quality of Product

Cybersecurity-effect on systems can impact product quality, maintenance, and systems monitoring. Impacts can include loss of confidentiality and integrity such as disclosure of status information or test results to unintended parties. Organizations should:

- develop systems and train personnel to acknowledge potential cybersecurity risk vectors in maintaining product quality
- plan for quality measures including:
  - testing
  - preventive maintenance
  - remediation
  - ongoing situational awareness
- manage prominent and increasing role of automated systems in maintaining control of product during safe transport.

Identify	***Assessing risks and understanding parameters about product are important to maintain product quality.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Asset Management	**ID.AM-5**	ID.AM-1, ID.AM-3, ID.AM-6
Risk Assessment	**ID.RA-5**	ID.RA-1

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Asset Management	ID.AM-1: Physical devices and systems within the organization are inventoried	*Rationale only provided for High Priority Subcategories*	• CCS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8	ACM-1a, -1c, -1e, -1f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Asset Management	ID.AM-3: Organizational communication and data flows are mapped	*Rationale only provided for High Priority Subcategories*	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8	RM-2g, AC-1e
Asset Management	**ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value**	**Potential product quality impacts of MBLT operations resources are necessary factors to consider when prioritizing resources. Resource prioritization informs how Cybersecurity Framework functions are performed with a strong emphasis on protection activities. Regular reviews and updates to resource prioritization based on changes to the device and system inventory support organizations in focusing expenditures where they are most impactful.**	• **COBIT 5 APO03.03, APO03.04, BAI09.02** • **ISA 62443-2-1:2009 4.2.3.6** • **ISO/IEC 27001:2013 A.8.2.1** • **NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14**	**ACM-1a, -1b, -1c, -1d**
Asset Management	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO01.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11	WM-1a, -1b, -1c

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Risk Assessment	ID.RA-1: Asset vulnerabilities are identified and documented	*Rationale only provided for High Priority Subcategories*	• CCS CSC 4 • COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04 • ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • ISO/IEC 27001:2013 A.12.6.1, A.18.2.3 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	TVM-2a, 2b, -2d, -2e, -2f, 2i, -2j, -2k, -2l, -2m, RM-1c, -2j
Risk Assessment	**ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk**	**Understanding threats and vulnerabilities related to specific IT and OT technologies employed in an organization's operating environment for MBLT operations, as well as how the unique combination(s) of them affect the organization's risk posture, is necessary for conducting thorough and accurate risk assessments. Examining threats and vulnerabilities in the context of the organization's particular operating environment produces a realistic picture of the likelihood of a risk being realized and the potential impacts that may affect the organization's ability to maintain product quality, and also provides input into monitoring plans.**	• **COBIT 5 APO12.02** • **ISO/IEC 27001:2013 A.12.6.1** • **NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16**	**RM-1c, 2j, TVM-2m**

Protect	***Appropriate physical and information security requires training and technology to protect the product.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Awareness and Training	**PR.AT-5**	PR.AT-1, PR.AT-3
Protective Technology	**PR.PT-4**	PR.PT-1, PR.PT-3

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-1: All users are informed and trained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, BAI05.07 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.7.2.2 • NIST SP 800-53 Rev. 4 AT-2, PM-13	WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i
Awareness and Training	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	**PR.AT-5: Physical and information security personnel understand roles & responsibilities**	**Personnel involved in MBLT operations must understand the policies and procedures that are in place to address IT and OT cybersecurity risks that may result in issues with maintaining product quality in the context of their individual roles and responsibilities. While a full understanding of enterprise risk management and cybersecurity strategies is not necessary or even important for all job roles, personnel must have an understanding of how to prioritize responsibilities as needed.**	• **CCS CSC 9** • **COBIT 5 APO07.03** • **ISA 62443-2-1:2009 4.3.2.4.2** • **ISO/IEC 27001:2013 A.6.1.1, A.7.2.2** • **NIST SP 800-53 Rev. 4 AT-3, PM-13**	**WM-1a, -1b, -1c, -1d, -1e, -1f, -1g**
Protective Technology	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	*Rationale only provided for High Priority Subcategories*	• CCS CSC 14 • COBIT 5 APO11.04 • ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 • ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 • ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 • NIST SP 800-53 Rev. 4 AU Family	SA-1a, -1b, -1c, -2a, -2e, -3d, -4e, -4f, -4g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 • ISO/IEC 27001:2013 A.9.1.2 • NIST SP 800-53 Rev. 4 AC-3, CM-7	IAM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h, -2i

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Protective Technology	**PR.PT-4: Communications and control networks are protected**	**Communications and control networks provide logical, non-local access to MBLT operations assets. This access is capable of providing useful operational and management capabilities, and can also be a source of great vulnerability if not well protected. Unauthorized access to communications and control networks may result in assets being manipulated in unpredictable ways, potentially resulting in product quality issues.**	• **CCS CSC 7** • **COBIT 5 DSS05.02, APO13.01** • **ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6** • **ISO/IEC 27001:2013 A.13.1.1, A.13.2.1** • **NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7**	**CPM-3a, -3b, -3c, -3d**

Detect	***Detecting anomalies and events is critical to maintaining quality of bulk liquid products.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Anomalies and Events	**DE.AE-2**	DE.AE-1, DE.AE-3, DE.AE-4, DE.AE-5

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	SA-2a

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Anomalies and Events	**DE.AE-2: Detected events are analyzed to understand attack targets and methods**	**Determining whether and how MBLT operational components are attacked provides insight into operational impacts that may affect the organization's ability to maintain product quality.**	• **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8** • **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2** • **ISO/IEC 27001:2013 A.16.1.1, A.16.1.4** • **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI4**	**IR-1f, -2i, -3h**
Anomalies and Events	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	*Rationale only provided for High Priority Subcategories*	• ISA 62443-3-3:2013 SR 6.1 • NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR5, IR-8, SI-4	IR-1e, -1f, -2i
Anomalies and Events	DE.AE-4: Impact of events is determined	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI 4	IR-2b, -2d, -2g, -2j, TVM-1d
Anomalies and Events	DE.AE-5: Incident alert thresholds are established	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	IR-2a, -2d, -2g, TVM-1d, SA-2d, RM-2j

Respond	***Appropriate response planning is critical to maintain quality of bulk liquid products.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Response Planning	N/A	RS.RP-1

Detailed Specifications	Optional Resources

Category	Subcategory	Rationale for High Priority	Cybersecurity Framework-based Informative References	C2M2 Practices
Response Planning	RS.RP-1: Response plan is executed during or after an event	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI01.10 • CCS CSC 18 • ISA 62443-2-1:2009 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR8	IR-3d

Recover	***N/A***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
N/A	N/A	N/A

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
N/A	N/A	N/A	N/A	N/A

A-6 Mission Objective 6: Meet HR Requirements

Mission Objective 6: Meet HR Requirements

Cybersecurity-effect (security and privacy) on operational systems impacting security and trust of personnel and their information. Organizations should:

- ensure appropriate governance, plans, procedures and oversight of connected HR systems and data including roles of employee managers in training and awareness
- understand risks, identify and train personnel on interdependence of cybersecurity with operational responsibilities and connections to source HR systems
- implement procedures to protect data in systems that contain personnel information
- implement Detect/Respond/Remediate activities where cybersecurity adversely affects personnel or personnel data.

Identify	***HR requirements are closely aligned to governance requirements. Managing the workforce requires an understanding of internal and external security obligations.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Governance	**ID.GV-2, ID.GV-3**	ID.GV-1

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Governance	ID.GV-1: Organizational information security policy is established	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO01.03, EDM01.01, EDM01.02 • ISA 62443-2-1:2009 4.3.2.6 • ISO/IEC 27001:2013 A.5.1.1 • NIST SP 800-53 Rev. 4 -1 controls from all families	CPM-2g, -5d, RM-3e

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Governance	**ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners**	**Operating certain IT and OT equipment necessitates an adequate degree of knowledge and experience, which can be demonstrated through the achievement of licenses, certifications, and other professional designations. In some cases, a current license is a condition for operating OT equipment. These requirements must be considered when defining and assigning security roles and responsibilities. Similarly, the associated access controls related Subcategories should be determined by the authorizations appropriate to the licensing level.**	• **COBIT 5 APO13.12** • **ISA 62443-2-1:2009 4.3.2.3.3** • **ISO/IEC 27001:2013 A.6.1.1, A.7.2.1** • **NIST SP 800-53 Rev. 4 PM-1, PS-7**	**WM-1a, -1b, -1c, -1e, -1f, -1g, -2d, -5b, ISC-2b**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Governance	**ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed**	**Various MBLT operational activities may be driven or influenced by multiple federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies, that govern information about the workforce that is collected and maintained by the organization. Protecting workforce information from loss, theft, or other compromises ensures the organization can meet HR requirements. Protecting workforce information also prevents harms to individuals, such as identity theft or embarrassment, and harms to the organization, such as diversion of resources away from operational objectives or employee distractions due to dealing with identify theft.**	• **COBIT 5 MEA03.01, MEA03.04** • **ISA 62443-2-1:2009 4.4.3.7**	**CPM-2k, IR-3n, RM-3f, -5f, AACM-4f, IAM-3f, TVM-3f, SA-4f, ISC-2f, EDM-3f, WM-5f**

Protect	***Personnel are often the first or second line of defense for an organization's resources. Aligning cybersecurity requirements to HR activities aids the organization in achieving compliance with internal policies and procedures, including completion of training requirements maintaining appropriate levels of access to resources.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Awareness and Training	**PR.AT-1**	PR.AT-4, PR.AT-5
Information Protection Processes & Procedures	**PR.IP-11**	PR.IP-1, PR.IP-4, PR.IP-5, PR.IP-9, PR.IP-10, PR.IP-12

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	**PR.AT-1: All users are informed an trained**	**Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity-related HR roles, responsibilities, and requirements necessary to support MBLT operations.**	• **CCS CSC 9** • **COBIT 5 APO07.03, BAI05.07** • **ISA 62443-2-1:2009 4.3.2.4.2** • **ISO/IEC 27001:2013 A.7.2.2** • **NIST SP 800-53 Rev. 4 AT-2, PM-13**	WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i
	PR.AT-2: Privileged users understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.02, DSS06.03 • ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-4: Senior executives understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
Information Protection Processes & Procedures	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	*Rationale only provided for High Priority Subcategories*	• CCS CSC 3, 10 • COBIT 5 BAI10.01, BAI10.02, BAI10.03, BAI10.05 • ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3 • ISA 62443-3-3:2013 SR 7.6 • ISO/IEC 27001:2013 A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 • NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	ACM-2a, -2b, -2c, -2d, -2e
Information Protection Processes & Procedures	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.9 • ISA 62443-3-3:2013 SR 7.3, SR 7.4 • ISO/IEC 27001:2013 A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 • NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9	PR-4a, -4b

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	ACM-4f, -3f
Information Protection Processes & Procedures	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS04.03 • ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1 • ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2 • NIST SP 800-53 Rev. 4 CP-2, IR-8	IR-3f, 3k, 3m, -4c, -4d, -4f, -4i, -4j, -5a, -5b, -5d, -5e, -5f, -5g, -5h, -5i, TVM-1d, RM-1c
Information Protection Processes & Procedures	PR.IP-10: Response and recovery plans are tested	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	IR-3e, 3k, -4f, -4i, -4j

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	**PR.IP-11: Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening)**	**MBLT operations rely on personnel to operate and maintain HR assets, and personnel that fulfill HR requirements commonly have privileged access to sensitive workforce information, such as salary information and performance reviews. Including cybersecurity in human resources practices helps ensure that the right people have access to the right assets at the right times through activities such as: screening personnel against applicable integrity and knowledge conditions, provisioning and de-provisioning access to assets based on role changes, terminating access when no longer required, and holding personnel accountable for understanding and meeting their HR-related roles and responsibilities. Including cybersecurity in HR practices also provides an avenue for enforcing training requirements and employing formal sanctions for failing to comply with HR-related policies and procedures.**	• **COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05** • **ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3** • **ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4** • **NIST SP 800-53 Rev. 4 PS Family**	**WM-2a, -2b, -2c, -2d, -2e, -2f, -2g, -2h**
Information Protection Processes & Procedures	PR.IP-12: A vulnerability management plan is developed and implemented	*Rationale only provided for High Priority Subcategories*	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	TVM-3a, -3e

Detect	***HR activities provide useful inputs for detecting anomalies and events. Conversely, understanding the HR context behind anomalies and events aids in determining potential and actual impacts of events.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Anomalies and Events	**DE.AE-2**	DE.AE-1, DE.AE-4, DE.AE-5

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Anomalies and Events	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS03.01 • ISA 62443-2-1:2009 4.4.3.3 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4	SA-2a
Anomalies and Events	**DE.AE-2: Detected events are analyzed to understand attack targets and methods**	**Determining whether and how MBLT HR components are attacked provides insight into impacts that may affect the organization's ability to maintain HR requirements.**	• **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8** • **ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2** • **ISO/IEC 27001:2013 A.16.1.1, A.16.1.4** • **NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI4**	**IR-1f, -2i, -3h**
Anomalies and Events	DE.AE-4: Impact of events is determined	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI 4	IR-2b, -2d, -2g, TVM-1d, RM-2j

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Anomalies and Events	DE.AE-5: Incident alert thresholds are established	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.2.3.10 • NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8	IR-2a, -2d, -2g, -2j, TVM-1d, SA-2d

Respond	***Response capabilities help limit the impacts of a cybersecurity event on HR activities.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Communications	**RS.CO-2**	RS.CO-3
Mitigation	**RS.MI-3**	RS.MI-1, RS.MI-2

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Communications	RC.CO-2: Events are reported consistent with established criteria	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.6.1.3, A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8	IR-1a, -1b
Communications	RS.CO-3: Information is shared consistent with response plans	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.2 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR4, IR-8, PE-6, RA-5, SI-4	ISC-1a, 1b, -1c, -d, IR-3d, -3i, -3l
Mitigation	RS.MI-1: Incidents are contained	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4	IR-3b

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Mitigation	RS.MI-2: Incidents are mitigated	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10 • ISO/IEC 27001:2013 A.12.2.1, A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4	IR-3b
Mitigation	**RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks**	**When vulnerabilities that affect the organization's ability to meet HR requirements are discovered in the process of responding to a cybersecurity event, organizations must determine the most effective risk response based on known information about the vulnerabilities that led to the event. Depending on the severity of a vulnerably that impacts HR requirements and the cybersecurity events it can lead to, acceptance may not be an appropriate response. Decisions made for short-term event response may not be the long-term risk response once the organization is in the Recover phase.**	• **ISO/IEC 27001:2013 A.12.6.1** • **NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5**	**TVM-2c, -2f, -2g, -2m, -2n, RM-2j**

Recover	***N/A***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
N/A	N/A	N/A

Detailed Specifications	**Optional Resources**

Category	Subcategory	Rationale for High Priority	Cybersecurity Framework-based Informative References	C2M2 Practices
N/A	N/A	N/A	N/A	N/A

A-7 Mission Objective 7: Pass Required Audits/Inspections

Mission Objective 7: Pass Required Audits/Inspections

Developing systems and training personnel to demonstrate readiness and execution of established plans. Organizations should:

- review plans and conduct in-person inspections via various means including:
  - automated/cybersecurity interface testing
  - sensor testing
  - backup/resilience process evaluation
  - plan and testing of data exchange/reporting methods
- ensure confidentiality of sensitive data, plans, and procedures

Identify	***The business environment and governance practices shape the requirements organizations must meet order to pass required audits and inspections.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Business Environment	**ID.BE-5**	ID.BE-3, ID.BE-4
Governance	**ID.GV-3**	ID.GV-4

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Business Environment	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO02.01, APO02.06, APO03.01 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • NIST SP 800-53 Rev. 4 PM-11, SA-14	RM-1c, -3b

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Business Environment	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	*Rationale only provided for High Priority Subcategories*	• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 • NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14	ACM-1a, -1b, -1c, -1d, -1e, -1f, EDM-1a, -1c, -1e, -1g, RM-1c
Business Environment	**ID.BE-5: Resilience requirements to support delivery of critical services are established**	**The ability to pass audits and inspections is contingent upon the IT and OT systems that support MBLT operations running at an acceptable capacity with adequate controls, even after a cybersecurity event occurs. Establishing what is acceptable and adequate for an organization requires advanced planning and coordination with relevant stakeholders.**	• **COBIT 5 DSS04.02** • **ISO/IEC 27001:2013 A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1** • **NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14**	**IR-4a, -4b, -4c, -4e**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Governance	**ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed**	**Various MBLT operational activities may be driven or influenced by multiple federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies. Audits and inspections will be conducted against applicable drivers, including considerations for cybersecurity. Maintaining an acceptable state of audit or inspection readiness provides a reasonable foundation for addressing known risks, and also saves resources expended to prepare for and participate in audits and inspections.**	• **COBIT 5 MEA03.01, MEA03.04** • **ISA 62443-2-1:2009 4.4.3.7** • **ISO/IEC 27001:2013 A.18.1** • **NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)**	**CPM-2k, IR-3n, RM-3f, AACM-4f, IAM-3f, TVM-3f, SA-4f, ISC-2f, IR-5f, EDM-3f, WM-5f**
Governance	ID.GV-4: Governance and risk management processes address cybersecurity risks	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS04.02 • ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 • NIST SP 800-53 Rev. 4 PM-9, PM-11	RM-2a, -2b, -2h, -3e, -1c, -1e

Protect	***The ability to demonstrate adequate protection of resources and equipment during an inspection or audit relies heavily on well documented policies and procedures and adequate awareness and training activities.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Awareness and Training	**PR.AT-1**	PR.AT-3, PR.AT-4, PR.AT-5
Information Protection Processes & Procedures	**PR.IP-9**	PR.IP-2, PR.IP-5, PR.IP-10, PR.IP-11, PR.IP-12

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	**PR.AT-1: All users are informed and trained**	**Periodic training, in conjunction with regular awareness activities, is an effective way to promote a culture of cybersecurity and maintain awareness of the cybersecurity-related IT and OT roles, responsibilities, and requirements necessary to support MBLT operations.**	• **CCS CSC 9** • **COBIT 5 APO07.03, BAI05.07** • **ISA 62443-2-1:2009 4.3.2.4.2** • **ISO/IEC 27001:2013 A.7.2.2** • **NIST SP 800-53 Rev. 4 AT-2, PM-13**	WM-3a, -4a, -3b, -3c, -3d, -3g, -3h, -3i
Awareness and Training	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03, APO10.04, APO10.05 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 PS-7, SA-9	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
Awareness and Training	PR.AT-4: Senior executives understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Awareness and Training	PR.AT-5: Physical and information security personnel understand roles & responsibilities	*Rationale only provided for High Priority Subcategories*	• CCS CSC 9 • COBIT 5 APO07.03 • ISA 62443-2-1:2009 4.3.2.4.2 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 • NIST SP 800-53 Rev. 4 AT-3, PM-13	WM-1a, -1b, -1c, -1d, -1e, -1f, -1g
Information Protection Processes & Procedures	PR.IP-2: A System Development Life Cycle to manage systems is implemented	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3 • ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8	ACM-3d
Information Protection Processes & Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	ACM-4f, RM-3f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	**PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed**	**MBLT operations response and recovery plans define the degree of IT and OT operations necessary to return to a desired minimum state of operations after a cybersecurity event. Developing and managing these plans in coordination with incident response processes ensures that the necessary activities occur when a cybersecurity event is identified. Instituting processes to manage response and recovery plans ensures they are periodically updated, allowing the organization to maintain an acceptable level of readiness for audits and inspections.**	• **COBIT 5 DSS04.03** • **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1** • **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2** • **NIST SP 800-53 Rev. 4 CP-2, IR-8**	**IR-3f, 3k, -3m, 4c, -4d, -4f, -4i, 4j, -5a, -5b, -5c, -5e, -5f, -5g, -5h, -5i, TVM-1d, RM-1c**
Information Protection Processes & Procedures	PR.IP-10: Response and recovery plans are tested	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.17.1.3 • NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14	IR-3d, 3k, -4f, -4i, -4j
Information Protection Processes & Procedures	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 • ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 • ISO/IEC 27001:2013 A.7.1.1, A.7.3.1, A.8.1.4 • NIST SP 800-53 Rev. 4 PS Family	WM-2a, -2b, -2c, -2d, -2e, -1f, -1g, -1h

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	PR.IP-12: A vulnerability management plan is developed and implemented	*Rationale only provided for High Priority Subcategories*	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	TVM-3a, -3e

Detect	***N/A***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
N/A	N/A	N/A

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
N/A	N/A	N/A	N/A	N/A

Respond	***When organizations experience a cybersecurity events, the ability to swiftly and effectively respond directly influences their ability to pass future inspections or audits.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Mitigation	**RS.MI-2**	RS.MI-1, RS.MI-3
Improvements	**RS.IM-1**	RS.IM-2

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Mitigation	RS.MI-1: Incidents are contained	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.3.4.5.6 • ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4 • ISO/IEC 27001:2013 A.16.1.5 • NIST SP 800-53 Rev. 4 IR-4	IR-3h
Mitigation	**RS.MI-2: Incidents are mitigated**	**Unmitigated IT and OT cybersecurity-related events may result in safety, operational, or compliance issues that limit or prevent an organization's ability to pass an audit or inspection.**	• **ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10** • **ISO/IEC 27001:2013 A.12.2.1, A.16.1.5** • **NIST SP 800-53 Rev. 4 IR-4**	**IR-3b**
Mitigation	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	*Rationale only provided for High Priority Subcategories*	• ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5	TVM-2c, -2f, -2g, -2m, -2n, RM-2j
Improvements	**RS.IM-1: Recovery plans incorporate lessons learned**	**Lessons learned from responding to a cybersecurity event provide valuable feedback for policy, procedural, and operational improvements that prevent or reduce adverse impacts to MBLT operations and aid the organization in maintaining an acceptable level of readiness for audits and inspections.**	• **COBIT 5 BAI01.13** • **ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4** • **ISO/IEC 27001:2013 A.16.1.6** • **NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8**	**IR-3h**
Improvements	RS.IM-2: Response strategies are updated		• NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8	IR-3h, -3k

Recover	*N/A*	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
N/A	N/A	N/A

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
N/A	N/A	N/A	N/A	N/A

A-8 Mission Objective 8: Obtain Timely Vessel Clearance

Mission Objective 8: Obtain Timely Vessel Clearance

Assure cybersecurity dimension of systems that can impact readiness and operational preparedness. Organizations should:

- demonstrate and share documents, data and other items to assure safe and secure entry into a port environment
- ensure confidentiality of sensitive data, plans, and procedures, particularly personnel data and documents

Identify	***The business environment and governance practices shape the requirements organizations must meet order to obtain timely vessel clearance.***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Business Environment	**ID.BE-4**	ID.BE-3
Governance	**ID.GV-3**	ID.GV-2

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Business Environment	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO02.01, APO02.06, APO03.01 • ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6 • NIST SP 800-53 Rev. 4 PM-11, SA-14	RM-3b, -1c

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Business Environment	**ID.BE-4: Dependencies and critical functions for delivery of critical services are established**	**Dependency and criticality analysis informs protection activities that are critical to maintaining the MBLT operational activities required for timely vessel clearance. Establishing those dependencies and critical functions is a process that includes identifying critical organizational missions, their associated MBLT operational functions and activities, and traceability to specific assets.**	• ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3 • NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11, PM-8, SA-14	**ACM-1a, -1b, -1c, -1d, -1e, -1f, EDM-1a, -1c, -1e, -1g**
Governance	ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev. 4 PM-1, PS-7	WM-1a, -1b, -1c, -1e, -1f, -1g, -2d, -5b, ISC-2b
Governance	**ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed**	**Various MBLT operational activities may be driven or influenced by multiple federal laws, Executive Orders, directions, policies, and regulations, including internal organizational policies. Demonstrating adherence to those requirements enables efficient and timely vessel clearance.**	• COBIT 5 MEA03.01, MEA03.04 • ISA 62443-2-1:2009 4.4.3.7 • ISO/IEC 27001:2013 A.18.1 • NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)	**CPM-2k, IR-3n, -5f, RM-3f, AACM-4f, IAM-3f, TVM-3f, SA-4f, ISC-2f, EDM-3f, WM-5f**

Protect	***The ability to demonstrate a state of readiness and operational preparedness relies heavily***

	on well documented policies and procedures, and adequate awareness and training activities.	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Access Control	N/A	PR.AC-1
Data Security	**PR.DS-6**	PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-5
Information Protection Processes & Procedures	**PR.IP-9**	PR.IP-2, PR.IP-5, PR.IP-12

Detailed Specifications			**Optional Resources**	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users	*Rationale only provided for High Priority Subcategories*	• CCS CSC 16 • COBIT 5 DSS05.04, DSS06.03 • ISA 62443-2-1:2009 4.3.3.5.1 • ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 • ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 • NIST SP 800-53 Rev. 4 AC-2, IA Family	IAM-1a, -1b, -1c, -1d, -1e, -1f, -1g, RM-1c
Data Security	PR.DS-1: Data-at-rest is protected	*Rationale only provided for High Priority Subcategories*	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev. 4 SC-28	TVM-1c, -2c

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Data Security	PR.DS-2: Data-in-transit is protected	*Rationale only provided for High Priority Subcategories*	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 SC-8	TVM-1c, -2c
Data Security	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	*Rationale only provided for High Priority Subcategories*	• COBIT 5 BAI09.03 • ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1 • ISA 62443-3-3:2013 SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7 • NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16	ACM-3a, -3b, -3c, -3d, -3f, -4a, -4b, -4c, -4d, -4e, -4f, -4g

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Data Security	PR.DS-5: Protections against data leaks are implemented	*Rationale only provided for High Priority Subcategories*	• CCS CSC 17 • COBIT 5 APO01.06 • ISA 62443-3-3:2013 SR 5.2 • ISO/IEC 27001:2013 A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	TVM-1c, -2c, CPM-3b
Data Security	**PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity**	**Unauthorized changes to IT or OT software, firmware, or information that support MBLT operations may result in safety, operational, or compliance issues that limit or prevent an organization's ability to obtain timely vessel clearance. Determining appropriate triggers and frequency for conducting integrity checks and how to respond for assets enables organizations to respond efficiently and effectively when integrity-related cybersecurity events are identified.**	• **ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4, SR 3.8** • **ISO/IEC 27001:2013 A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3** • **NIST SP 800-53 Rev. 4 SI-7**	**SA-2e, -2i**

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	PR.IP-2: A System Development Life Cycle to manage systems is implemented	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.01 • ISA 62443-2-1:2009 4.3.4.3.3 • ISO/IEC 27001:2013 A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 • NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA10, SA-11, SA-12, SA-15, SA-17, PL-8	ACM-3d
Information Protection Processes & Procedures	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	*Rationale only provided for High Priority Subcategories*	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 • ISO/IEC 27001:2013 A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 • NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18	ACM-4f, -3f

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Information Protection Processes & Procedures	**PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed**	**MBLT operations response and recovery plans define the degree of IT and OT operations necessary to return to a desired minimum state of operations after a cybersecurity event. Developing and managing these plans in coordination with incident response processes ensures that the necessary activities occur when a cybersecurity event is identified. Instituting processes to manage response and recovery plans ensures they are periodically updated, allowing the organization to maintain an acceptable level of readiness for obtaining timely vessel clearance.**	• **COBIT 5 DSS04.03** • **ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1** • **ISO/IEC 27001:2013 A.16.1.1, A.17.1.1, A.17.1.2** • **NIST SP 800-53 Rev. 4 CP-2, IR-8**	**IR-3f, 3k, -3m, 4c, -4d, -4f, -4i, 4j, -5a, -5b, -5c, -5e, -5f, -5g, -5h, -5i,** **TVM-1d,** **RM-1c**
Information Protection Processes & Procedures	PR.IP-12: A vulnerability management plan is developed and implemented	*Rationale only provided for High Priority Subcategories*	• ISO/IEC 27001:2013 A.12.6.1, A.18.2.2 • NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2	TVM-3a, -3e

Detect	***Detection processes must comply with applicable rules and regulations***	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Detection Processes	**DE.DP-2**	DE.DP-1, DE.DP-3, DE.DP-4, DE.DP-5

Detailed Specifications	**Optional Resources**

Category	Subcategory	Rationale for High Priority	Cybersecurity Framework-based Informative References	C2M2 Practices
Detection Processes	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	*Rationale only provided for High Priority Subcategories*	• CCS CSC 5 • COBIT 5 DSS05.01 • ISA 62443-2-1:2009 4.4.3.1 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14	WM-1a, -1d, -1f
Detection Processes	DE.DP-2: Detection activities comply with all applicable requirements	*Rationale only provided for High Priority Subcategories*	• ISA 62443-2-1:2009 4.4.3.2 • ISO/IEC 27001:2013 A.18.1.4 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4	IR-1d, 5a, -1g, -5f, TVM-1d, RM-1c, -2j
Detection Processes	DE.DP-3: Detection processes are tested	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4	IR-3e, -3j
Detection Processes	DE.DP-4: Event detection information is communicated to appropriate parties	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, RA-5, SI-4	IR-1b, -3c, -3n, ISC-1a, -1c, -1d, -1h, -1j
Detection Processes	DE.DP-5: Detection processes are continuously improved	*Rationale only provided for High Priority Subcategories*	• COBIT 5 APO11.06, DSS04.05 • ISA 62443-2-1:2009 4.4.3.4 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14	IR-3h, -3k
Respond		***N/A***		

Categories	High Priority Subcategories	Moderate Priority Subcategories
N/A	N/A	N/A

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
N/A	N/A	N/A	N/A	N/A

Recover	*When organizations experience a cybersecurity events, their ability to recover directly influences their ability to demonstrate an acceptable state of readiness and operational preparedness for obtaining timely vessel clearance.*	
Categories	**High Priority Subcategories**	**Moderate Priority Subcategories**
Communications	N/A	RC.CO-3

Detailed Specifications			Optional Resources	
Category	**Subcategory**	**Rationale for High Priority**	**Cybersecurity Framework-based Informative References**	**C2M2 Practices**
Communications	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	*Rationale only provided for High Priority Subcategories*	• NIST SP 800-53 Rev. 4 CP-2, IR-4	IR-3d

Appendix B – Section by Section Review of 33 CFR 154-156

B-1 Bulk Liquid Transfer Facilities, 33 CFR 154

The United States Coast Guard regulates 'facilities transferring oil or hazardous material in bulk' under 33 CFR 154.

Subpart A

Subpart A, sections 154.100-154.120, provides general items such as applicability, definitions, alternatives, exemptions, letters of intent, and facility examinations.

No particular sections under this subpart apply to cybersecurity. Exemption rules and facility examination rules might come into play.

Subpart B

Subpart B, sections 154.300-154.325, call for the creation, evaluation and use of a facilities Operations Manual. This Manual is developed by the facilities operator and inspected by the USCG Captain of the Port (COTP)

The Operations Manual called for under this part describes the operating rules and equipment requirements for the facility. Operating rules can include interfacing with systems that have a cybersecurity component. Likewise, equipment in modern facilities is often managed by computer based interfaces that should be seen as a cyber-physical system.

The responsibilities of the personnel described under this part can include interacting with the computer and cyber based systems operating the facility and equipment. As such, assessment criteria can be useful to assist in determining whether sufficient cybersecurity controls are in place to protect the systems and equipment from purposeful or accidental misuse.

Section 154.310-312 describes the table of contents of the Operations Manual, amendments to the Operations Manual and procedures for examination.

Subpart C

Subpart C, sections 154.500-154.570, describe equipment requirements.

Most of this subpart does not have a cybersecurity component items such as monitoring devices.

Monitoring devices, section 154.525, may well be connected to alarm systems that may be compromised via cybersecurity threats.

Emergency shutdown, section 154.550, calls for connections to the facility that may be vulnerable to cybersecurity threats as well as communications systems that can be interrupted. Emergency shutdowns must be monitored to show shutdown within 30-60 seconds.

Communications, section 154.560, calls for continuous two-way communications to be available throughout the transfer process. This is allowed via radio devices as well. In either case, cybersecurity threats are possible against communications systems.

Subpart D

Subpart D, sections 154.700-154.750, describe facility operations.

Person in charge, section 154.710, relates to the training and qualifications of those managing bulk liquid transfer operations. It may have implications with the HR mission identified in the mapping below.

Safety requirements, section 154.735, mostly relates to equipment readiness to respond to safety needs.

Records, section 154.740, relates to documentation of people, processes, inspection certificates, prior shut downs, communications safety, and compliance with the Operations Manual procedures. If these records are maintained electronically they may be vulnerable to cybersecurity risks of compromise.

Subpart E

Subpart E, sections 154.800-154.850, describe vapor control systems.

Review, certification, and initial inspection, section 154.804 describes alarm and automatic control systems. The section also states that if a quantitative failure analysis is conducted certain standardized procedures should be followed. It also describes the certification and inspection process. Automated data collection processes used in these analyses may be vulnerable to cybersecurity risks.

Vapor control systems, general, section 154.804, describes liquid level sensors connected to an alarm system and remotely operated shutoff valves. Either of these systems may be vulnerable to cybersecurity threats.

Vapor line connections, section 154.810, calls for detection systems that can shutdown components of the system and alarm systems. Either of these systems may be vulnerable to cybersecurity threats.

Facility requirements for vessel liquid overfill protection, section 154.812, includes sensors that may be connected to alarm and shutdown systems. It includes a remotely operated cargo vapor shutoff valve, overfill signals, automated testing of alarms and automated shutdown systems.

Facility requirements for vessel vapor overpressure and vacuum protection, section 154.814, includes pressure sensors, alarms, emergency shutdown, remote closure devices, and vacuum relief valves that may be vulnerable to cybersecurity threats.

Fire, explosion, and detonation protection, section 154.820 includes oxygen analyzers, various systems including alarm systems that may be vulnerable to cybersecurity threats.

Inerting, enriching, and diluting systems, section 154.824, include monitoring, vapor concentration analyzers, oxygen analyzers, hydrocarbon analyzers, volumetric measurement guided by API

Recommended Practice 550 as well as sampling systems, response times, alarm systems and shutoff valves that may be vulnerable to cybersecurity threats.

Vapor recovery and vapor destruction units, section 154.828 utilize detectors, arrestors, and remotely operated shutoff valves that may be vulnerable to cybersecurity threats.

Operational requirements, section 154.850, calls for testing of alarms, measurements, analyzers, shutdown systems, and flame detector systems that may be vulnerable to cybersecurity threats.

Subpart F

Subpart F, sections 154.1010-154.1075, describe response plans for oil facilities. The section describes in great detail the contents of the response plan, and requirements for authorization processes, personnel, procedures, equipment, communication, escalation, timing, training, testing, response exercises, inspection, maintenance, review and appeals processes. The system is appropriately response based and has little focus on systems with a cybersecurity component.

Subparts G-I

Subpart G-I, sections 154.1110-154.1325, describe additional response plans for Trans-Alaska pipeline facilities, facilities handling animal fats and vegetable oils, and facilities handling non-petroleum oil.

Subpart G, sections 154.1100-1140, adds requirements to subpart F for Trans Alaska Pipeline Authorization Act facilities operating in Prince William Sound, Alaska. It adds extra testing and prepositioned response equipment requirements beyond subpart F.

Subpart H, sections 154.1210-1240, adds requirements to subpart F for animal fats and vegetable oil facilities. It covers facility classification, submission requirements, plan development and evaluation criteria, equipment, and response resources. It modifies the rule for reporting corporate organizational structure and requires the response plan resources identified in this subpart be able to manage a worst case discharge.

Subpart I, sections 134.1310-1325 adds requirements to subpart F for non-petroleum oil facilities. It covers the planning process aspects of the response plan preparation. It includes procedures and strategies for worst case discharge, geography specific adaptation, equipment and devices, firefighting, and the use of dispersants.

The items in subparts G-I concentrate on response planning and have little focus on systems with a cybersecurity component.

Appendix A covers detonation flame arrestors.

Appendix B covers tank vent flame arrestors.

Appendix C covers response resources for facility response plans.

Appendix D covers training for oil spill response plans.

B-2 Oil and Hazardous Materials for Vessels, 33 CFR 155

The United States Coast Guard regulates 'oil or hazardous material pollution prevention regulations for vessels' under 33 CFR 155.

Subpart A, sections 155.100-155.140, covers general issues.

Subpart B, sections 155.200-490, covers vessel equipment.

Subpart C, sections 155.700-820, covers transfer personnel, procedures, equipment, and records.

Subpart D, sections 155.1010-155.1070, covers tank vessel response plans for oil.

Subpart E, sections 155.1110-155.1150, covers additional response plan requirements for tankers loading cargo at a trans-Alaska pipeline facility.

Subpart F, sections 155.1210-155.1230, covers additional response plan requirements for vessels carrying animal fats and vegetable oils.

Subpart G, sections 155.2210-155.2230, covers additional response plan requirements for vessels carrying non-petroleum oils.

Subpart I, sections 155.4010-155.4055, covers salvage and marine firefighting.

B-3 Oil and Hazardous Material Transfer Operations, 33 CFR 156

The United States Coast Guard regulates 'oil and hazardous material transfer operations' under 33 CFR 156.

Subpart A

Subpart A, sections 156.100-156.170 covers oil and hazardous material transfer operations. 156.100 covers the applicability of the section. 156.105 covers definitions and refers to 154.105 for those definitions. Section 156.107 allows alternative procedures, methods, or equipment upon the approval of the COTP. Section 156.110 covers exemptions as permitted by the Assistant Commandant for Marine Safety, Security, and Environmental Protection or the District Commander. Section 156.111 includes certain information by reference. Section 156.112 covers the issuing of suspension orders by the COTP or OCMI to suspend the transfer operations. Section 156.113 covers compliance with suspension orders. Section 156.114 limits the person in charge to be only in charge of one vessel's transfer operations at a time and not be in charge of both a vessel and facility except if allowed by the COTP. Section 156.118 requires 4-hour notice to the COTP before transfer operations begin. Section 156.120 identifies requirements for beginning a transfer. Section 156.125 covers discharge cleanup. Section 156.130 covers connections and couplings. Section 156.150 covers declarations of inspections. Section 156.160 covers supervision by the person in charge. Section 156.170 covers equipment tests and inspections.

Subpart B

Subpart B, sections 156.200-156.230 covers special requirements for lightering of oil and hazardous cargoes. Section 156.200 covers applicability of the subpart and related regulations. Section 156.205 covers definitions. It defines lightering as, “the transfer of a cargo of oil or hazardous material in bulk from one vessel to another.” Section 156.210 covers the general requirements for transfer of oil or hazardous materials. Section 156.215 requires pre-arrival notices of at least 24 hours. Section 156.220 covers the reporting of incidents. Section 156.225 covers lightering zone designation. Section 156.230 covers factors for designating a lightering zone.

Subpart C

Subpart C, sections 156.300-156.330 covers lightering zones and operational requirements for the Gulf of Mexico. Section 156.300 identifies the coordinates of the lightering zones. Section 156.310 identifies prohibited areas. Section 156.320 covers maximum operating conditions for winds and waves. Section 156.330 covers lightering operations.

Appendix C – Industry Cybersecurity Processes & Profile Mappings

C-1 Energy Sector Cybersecurity Efforts and the DOE C2M2 Program

Energy Sector Cybersecurity

In the last decade NIST has interacted with industry as energy networks become more than mere power delivery systems. As part of the development of the Smart Grid, NIST has worked with industry to develop a series of documents supporting the secure and reliable delivery of Smart Grid services with appropriate security and privacy.[24] It has established a standing Smart Grid Advisory Committee and works with the Smart Grid Interoperability Panel.

During the last several years, research has also focused on the impact of cybersecurity risks on physical systems beyond SCADA, ICS and Smart Grid. Research in this area has been given the term Cyber-Physical Systems, CPS. NIST held a workshop on CPS in August of 2014[25] and again in April 2015.[26] Related to the workshops, a set of work groups were established to support development of use cases, manage security and privacy issues, and to deal with issues specific to timing controls. This Cyber-Physical Systems Public Working Group released a draft CPS Framework to evaluate CPS systems and the risks they face.[27] The Industrial Internet Consortium has also had an active discussion regarding CPS security[28], and has released a reference architecture.

DOE Cybersecurity

The Department of Energy has worked with industry to develop the *Energy Sector Cybersecurity Framework Implementation Guidance*[29] document. Additionally, the DOE has developed the Cybersecurity Capability Maturity Model (C2M2). It describes the C2M2 program as:

"The Cybersecurity Capability Maturity Model (C2M2) program is a public-private partnership effort that was established as a result of the Administration's efforts to improve electricity subsector cybersecurity capabilities, and to understand the cybersecurity posture of the grid. The C2M2 helps organizations—regardless of size, type, or industry—evaluate, prioritize, and improve their own cybersecurity capabilities.

The model focuses on the implementation and management of cybersecurity practices associated with the operation and use of information technology and operational technology assets and the environments in which they operate."[30]

---

[24] NIST, Smart Grid landing page http://www.nist.gov/smartgrid/

[25] NIST, Cyber-Physical Systems Public Working Group Workshop, http://www.nist.gov/cps/cps-pwg-workshop.cfm

[26] NIST, Cyber-Physical Systems Public Working Group (CPS-PWG) Workshop – April 2015, http://nist.gov/cps/cps-pwg-workshop-april-2015.cfm

[27] Cyber-Physical Systems Public Working Group, draft *Cyber-Physical Systems Framework*, September 2015, www.cpspwg.org and https://pages.nist.gov/cpspwg

[28] Industrial Internet Consortium Security Working Group, http://www.iiconsortium.org/wc-security.htm

[29] http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

Further, DOE has adapted the C2M2 program for the oil and natural gas subsector. It describes the additional benefit of the ONG-C2M2:

"The ONG-C2M2 includes the core C2M2 as well as additional reference material and implementation guidance specifically tailored for the oil and natural gas subsector."[31]

This MBLT Profile has used both the Implementation Guidance and the ONG-C2M2. By leveraging this existing body of work, the MBLT Profile utilizes existing industry capability and cross-reference tables to allow organizations who have already leveraged the DOE program to utilize that work here.

This Profile has also utilized its seven step process for Cybersecurity Framework implementation as described in the Implementation Guidance. The following is a copy of the Implementation Guidance's Appendix B.

Table C-1. Summary of Framework Use Steps

Step 1: Prioritize and Scope		
Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Threat information	1. Organization determines where it wants to apply the Framework to evaluate and potentially guide the improvement of the organization's cybersecurity capabilities	1. Framework usage scope
Step 2: Orient		
Inputs	Activities	Outputs
1. Framework usage scope 2. Risk management strategy	1. Organization identifies in-scope systems and assets (e.g., people, information, technology, and facilities) and the appropriate regulatory and Informative References (e.g., cybersecurity and risk management standards, tools, methods, and guidelines)	1. In-scope systems and assets 2. In-scope requirements (i.e., regulatory, company, organizational) 3. In-scope cybersecurity and risk management standards, tools, methods, and guidelines 4. Evaluation approach
Step 3: Create a Current Profile		
Inputs	Activities	Outputs
1. Evaluation approach 2. In-scope systems and assets 3. In-scope regulatory requirements 4. In-scope cybersecurity and risk management standards, tools, methods, and guidelines	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile 2. Current Implementation Tier
Step 4: Conduct a Risk Assessment		
Inputs	Activities	Outputs
1. Framework usage scope	1. Perform risk assessment for in-	1. Risk assessment reports

[30] http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program
[31] http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity

2. Risk management strategy 3. Organization-defined risk assessment approach 4. In-scope regulatory requirements 5. In-scope cybersecurity and risk management standards, tools, methods, and guidelines	scope portion of the organization	
Step 5: Create a Target Profile		
Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Organizational objectives 4. Risk management strategy 5. Risk assessment reports	1. Organization identifies goals that will mitigate risk commensurate with the risk to organizational and critical infrastructure objectives	1. Target Profile 2. Target Tier
Step 6: Determine, Analyze, and Prioritize Gaps		
Inputs	Activities	Outputs
1. Current Profile 2. Current Tier 3. Target Profile 4. Target Tier 5. Organizational objectives 6. Impact to critical infrastructure 7. Gaps and potential consequences 8. Organizational constraints 9. Risk management strategy 10. Risk assessment reports	1. Analyze gaps between current state and Target Profile in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) on actions 6. Prioritize actions (CBA and consequences) 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan
Step 7: Implement Action Plan		
Inputs	Activities	Outputs
1. Prioritized implementation plan	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks, metrics, and performance indicators 4. Report progress	1. Project tracking data 2. New security measures implemented

C-2 Cybersecurity Framework Informative References

Other critical infrastructure organizations have also developed Cybersecurity Framework Profiles. Examples include the electric power industry, the public water industry, the aviation industry, and the transportation industry. Some of the Profile work predates the development of the Cybersecurity Framework. Others have incorporated the Cybersecurity Framework into their Profile work. We review some of this work in our related *How To Guide*.

C-3 Mapping of Optional Resources

The Cybersecurity Framework appendix describing the Framework Core includes informative references from other security standards. They are replicated here.

Subcategory	Informative References from Cybersecurity Framework
ID.AM-1: Physical devices and systems within the organization are inventoried	· **CCS CSC** 1
	· **COBIT 5** BAI09.01, BAI09.02
	· **ISA 62443-2-1:2009** 4.2.3.4
	· **ISA 62443-3-3:2013** SR 7.8
	· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
	· **NIST SP 800-53 Rev. 4** CM-8
ID.AM-2: Software platforms and applications within the organization are inventoried	· **CCS CSC** 2
	· **COBIT 5** BAI09.01, BAI09.02, BAI09.05
	· **ISA 62443-2-1:2009** 4.2.3.4
	· **ISA 62443-3-3:2013** SR 7.8
	· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
	· **NIST SP 800-53 Rev. 4** CM-8
ID.AM-3: Organizational communication and data flows are mapped	· **CCS CSC** 1
	· **COBIT 5** DSS05.02
	· **ISA 62443-2-1:2009** 4.2.3.4
	· **ISO/IEC 27001:2013** A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8

Subcategory	Informative References from Cybersecurity Framework
ID.AM-4: External information systems are catalogued	· **COBIT 5** APO02.02
	· **ISO/IEC 27001:2013** A.11.2.6
	· **NIST SP 800-53 Rev. 4** AC-20, SA-9
ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· **COBIT 5** APO03.03, APO03.04, BAI09.02
	· **ISA 62443-2-1:2009** 4.2.3.6
	· **ISO/IEC 27001:2013** A.8.2.1
	· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· **COBIT 5** APO01.02, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.2.3.3
	· **ISO/IEC 27001:2013** A.6.1.1
	· **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
ID.BE-1: The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
	· **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2
	· **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01
	· **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01
	· **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6
	· **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3
	· **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established	· **COBIT 5** DSS04.02
	· **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
	· **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14
ID.GV-1: Organizational information security policy is established	· **COBIT 5** APO01.03, EDM01.01, EDM01.02
	· **ISA 62443-2-1:2009** 4.3.2.6
	· **ISO/IEC 27001:2013** A.5.1.1
	· **NIST SP 800-53 Rev. 4** -1 controls from all families
ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	· **COBIT 5** APO13.12
	· **ISA 62443-2-1:2009** 4.3.2.3.3
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1
	· **NIST SP 800-53 Rev. 4** PM-1, PS-7
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **COBIT 5** MEA03.01, MEA03.04
	· **ISA 62443-2-1:2009** 4.4.3.7
	· **ISO/IEC 27001:2013** A.18.1
	· **NIST SP 800-53 Rev. 4** -1 controls from all families (except PM-1)

Subcategory	Informative References from Cybersecurity Framework
ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** DSS04.02
	· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3
	· **NIST SP 800-53 Rev. 4** PM-9, PM-11
ID.RA-1: Asset vulnerabilities are identified and documented	· **CCS CSC** 4
	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04
	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12
	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
	· **ISO/IEC 27001:2013** A.6.1.4
	· **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5
ID.RA-3: Threats, both internal and external, are identified and documented	· **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04
	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
	· **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
ID.RA-4: Potential business impacts and likelihoods are identified	· **COBIT 5** DSS04.02
	· **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12
	· **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-9, PM-11, SA-14
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **COBIT 5** APO12.02
	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
ID.RA-6: Risk responses are identified and prioritized	· **COBIT 5** APO12.05, APO13.02
	· **NIST SP 800-53 Rev. 4** PM-4, PM-9
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	· **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02
	· **ISA 62443-2-1:2009** 4.3.4.2
	· **NIST SP 800-53 Rev. 4** PM-9
ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.3.2.6.5
	· **NIST SP 800-53 Rev. 4** PM-9
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **NIST SP 800-53 Rev. 4** PM-8, PM-9, PM-11, SA-14

Subcategory	Informative References from Cybersecurity Framework
PR.AC-1: Identities and credentials are managed for authorized devices and users	· **CCS CSC** 16
	· **COBIT 5** DSS05.04, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.3.5.1
	· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
	· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3
	· **NIST SP 800-53 Rev. 4** AC-2, IA Family
PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05
	· **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8
	· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3
	· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
PR.AC-3: Remote access is managed	· **COBIT 5** APO13.01, DSS01.04, DSS05.03
	· **ISA 62443-2-1:2009** 4.3.3.6.6
	· **ISA 62443-3-3:2013** SR 1.13, SR 2.6
	· **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **CCS CSC** 12, 15
	· **ISA 62443-2-1:2009** 4.3.3.7.3
	· **ISA 62443-3-3:2013** SR 2.1
	· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4
	· **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· **ISA 62443-2-1:2009** 4.3.3.4
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.8
	· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, SC-7
PR.AT-1: All users are informed and trained	· **CCS CSC** 9
	· **COBIT 5** APO07.03, BAI05.07
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.7.2.2
	· **NIST SP 800-53 Rev. 4** AT-2, PM-13
PR.AT-2: Privileged users understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.02, DSS06.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13

Subcategory	Informative References from Cybersecurity Framework
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.03, APO10.04, APO10.05
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
	· **NIST SP 800-53 Rev. 4** PS-7, SA-9
PR.AT-4: Senior executives understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.AT-5: Physical and information security personnel understand roles & responsibilities	· **CCS CSC** 9
	· **COBIT 5** APO07.03
	· **ISA 62443-2-1:2009** 4.3.2.4.2
	· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2,
	· **NIST SP 800-53 Rev. 4** AT-3, PM-13
PR.DS-1: Data-at-rest is protected	· **CCS CSC** 17
	· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS06.06
	· **ISA 62443-3-3:2013** SR 3.4, SR 4.1
	· **ISO/IEC 27001:2013** A.8.2.3
	· **NIST SP 800-53 Rev. 4** SC-28
PR.DS-2: Data-in-transit is protected	· **CCS CSC** 17
	· **COBIT 5** APO01.06, DSS06.06
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** SC-8
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4. 4.3.3.3.9, 4.3.4.4.1
	· **ISA 62443-3-3:2013** SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.7
	· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
PR.DS-4: Adequate capacity to ensure availability is maintained	· **COBIT 5** APO13.01
	· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
	· **ISO/IEC 27001:2013** A.12.3.1
	· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5

Subcategory	Informative References from Cybersecurity Framework
PR.DS-5: Protections against data leaks are implemented	· **CCS CSC** 17
	· **COBIT 5** APO01.06
	· **ISA 62443-3-3:2013** SR 5.2
	· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8
	· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3
	· **NIST SP 800-53 Rev. 4** SI-7
PR.DS-7: The development and testing environment(s) are separate from the production environment	· **COBIT 5** BAI07.04
	· **ISO/IEC 27001:2013** A.12.1.4
	· **NIST SP 800-53 Rev. 4** CM-2
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	· **CCS CSC** 3, 10
	· **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05
	· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3
	· **ISA 62443-3-3:2013** SR 7.6
	· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	· **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
PR.IP-2: A System Development Life Cycle to manage systems is implemented	· **COBIT 5** APO13.01
	· **ISA 62443-2-1:2009** 4.3.4.3.3
	· **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
	· **NIST SP 800-53 Rev. 4** SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8
PR.IP-3: Configuration change control processes are in place	· **COBIT 5** BAI06.01, BAI01.06
	· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3
	· **ISA 62443-3-3:2013** SR 7.6
	· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
	· **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
PR.IP-4: Backups of information are conducted, maintained, and tested periodically	· **COBIT 5** APO13.01
	· **ISA 62443-2-1:2009** 4.3.4.3.9
	· **ISA 62443-3-3:2013** SR 7.3, SR 7.4
	· **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2A.17.1.3, A.18.1.3
	· **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9

Subcategory	Informative References from Cybersecurity Framework
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **COBIT 5** DSS01.04, DSS05.05
	· **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
	· **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
	· **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
PR.IP-6: Data is destroyed according to policy	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4.3.4.4.4
	· **ISA 62443-3-3:2013** SR 4.2
	· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
	· **NIST SP 800-53 Rev. 4** MP-6
PR.IP-7: Protection processes are continuously improved	· **COBIT 5** APO11.06, DSS04.05
	· **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **COBIT 5** DSS04.03
	· **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1
	· **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2
	· **NIST SP 800-53 Rev. 4** CP-2, IR-8
PR.IP-10: Response and recovery plans are tested	· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11
	· **ISA 62443-3-3:2013** SR 3.3
	· **ISO/IEC 27001:2013** A.17.1.3
	· **NIST SP 800-53 Rev.4** CP-4, IR-3, PM-14
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
	· **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3
	· **ISO/IEC 27001:2013** A.7.1.1, A.7.3.1, A.8.1.4
	· **NIST SP 800-53 Rev. 4** PS Family
PR.IP-12: A vulnerability management plan is developed and implemented	· **ISO/IEC 27001:2013** A.12.6.1, A.18.2.2
	· **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	· **COBIT 5** BAI09.03
	· **ISA 62443-2-1:2009** 4.3.3.3.7
	· **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5
	· **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **COBIT 5** DSS05.04
	· **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8
	· **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1
	· **NIST SP 800-53 Rev. 4** MA-4

Subcategory	Informative References from Cybersecurity Framework
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CCS CSC** 14
	· **COBIT 5** APO11.04
	· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
	· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
	· **NIST SP 800-53 Rev. 4** AU Family
PR.PT-2: Removable media is protected and its use restricted according to policy	· **COBIT 5** DSS05.02, APO13.01
	· **ISA 62443-3-3:2013** SR 2.3
	· **ISO/IEC 27001:2013** A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
	· **NIST SP 800-53 Rev. 4** MP-2, MP-4, MP-5, MP-7
PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	· **COBIT 5** DSS05.02
	· **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
	· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
	· **ISO/IEC 27001:2013** A.9.1.2
	· **NIST SP 800-53 Rev. 4** AC-3, CM-7
PR.PT-4: Communications and control networks are protected	· **CCS CSC** 7
	· **COBIT 5** DSS05.02, APO13.01
	· **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
	· **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1
	· **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	· **COBIT 5** DSS03.01
	· **ISA 62443-2-1:2009** 4.4.3.3
	· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
	· **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4
	· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	· **ISA 62443-3-3:2013** SR 6.1
	· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
DE.AE-4: Impact of events is determined	· **COBIT 5** APO12.06
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI -4
DE.AE-5: Incident alert thresholds are established	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.2.3.10
	· **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8

Subcategory	Informative References from Cybersecurity Framework
DE.CM-1: The network is monitored to detect potential cybersecurity events	· **CCS CSC** 14, 16
	· **COBIT 5** DSS05.07
	· **ISA 62443-3-3:2013** SR 6.2
	· **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· **ISA 62443-2-1:2009** 4.3.3.3.8
	· **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· **ISA 62443-3-3:2013** SR 6.2
	· **ISO/IEC 27001:2013** A.12.4.1
	· **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
DE.CM-4: Malicious code is detected	· **CCS CSC** 5
	· **COBIT 5** DSS05.01
	· **ISA 62443-2-1:2009** 4.3.4.3.8
	· **ISA 62443-3-3:2013** SR 3.2
	· **ISO/IEC 27001:2013** A.12.2.1
	· **NIST SP 800-53 Rev. 4** SI-3
DE.CM-5: Unauthorized mobile code is detected	· **ISA 62443-3-3:2013** SR 2.4
	· **ISO/IEC 27001:2013** A.12.5.1
	· **NIST SP 800-53 Rev. 4** SC-18, SI-4. SC-44
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06
	· **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1
	· **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
DE.CM-8: Vulnerability scans are performed	· **COBIT 5** BAI03.10
	· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7
	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** RA-5
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	· **CCS CSC** 5
	· **COBIT 5** DSS05.01
	· **ISA 62443-2-1:2009** 4.4.3.1
	· **ISO/IEC 27001:2013** A.6.1.1
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
DE.DP-2: Detection activities comply with all applicable requirements	· **ISA 62443-2-1:2009** 4.4.3.2
	· **ISO/IEC 27001:2013** A.18.1.4
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14, SI-4

Subcategory	Informative References from Cybersecurity Framework
DE.DP-3: Detection processes are tested	· **COBIT 5** APO13.02
	· **ISA 62443-2-1:2009** 4.4.3.2
	· **ISA 62443-3-3:2013** SR 3.3
	· **ISO/IEC 27001:2013** A.14.2.8
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
DE.DP-4: Event detection information is communicated to appropriate parties	· **COBIT 5** APO12.06
	· **ISA 62443-2-1:2009** 4.3.4.5.9
	· **ISA 62443-3-3:2013** SR 6.1
	· **ISO/IEC 27001:2013** A.16.1.2
	· **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
DE.DP-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, DSS04.05
	· **ISA 62443-2-1:2009** 4.4.3.4
	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RS.RP-1: Response plan is executed during or after an event	· **COBIT 5** BAI01.10
	· **CCS CSC** 18
	· **ISA 62443-2-1:2009** 4.3.4.5.1
	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
RS.CO-1: Personnel know their roles and order of operations when a response is needed	· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
	· **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1
	· **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
RS.CO-2: Events are reported consistent with established criteria	· **ISA 62443-2-1:2009** 4.3.4.5.5
	· **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2
	· **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
RS.CO-3: Information is shared consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.2
	· **ISO/IEC 27001:2013** A.16.1.2
	· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.5
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **NIST SP 800-53 Rev. 4** PM-15, SI-5
RS.AN-1: Notifications from detection systems are investigated	· **COBIT 5** DSS02.07
	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
	· **ISA 62443-3-3:2013** SR 6.1
	· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5
	· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

Subcategory	Informative References from Cybersecurity Framework
RS.AN-2: The impact of the incident is understood	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4
RS.AN-3: Forensics are performed	· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
	· **ISO/IEC 27001:2013** A.16.1.7
	· **NIST SP 800-53 Rev. 4** AU-7, IR-4
RS.AN-4: Incidents are categorized consistent with response plans	· **ISA 62443-2-1:2009** 4.3.4.5.6
	· **ISO/IEC 27001:2013** A.16.1.4
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
RS.MI-1: Incidents are contained	· **ISA 62443-2-1:2009** 4.3.4.5.6
	· **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4
	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** IR-4
RS.MI-2: Incidents are mitigated	· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10
	· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5
	· **NIST SP 800-53 Rev. 4** IR-4
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **ISO/IEC 27001:2013** A.12.6.1
	· **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
RS.IM-1: Response plans incorporate lessons learned	· **COBIT 5** BAI01.13
	· **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4
	· **ISO/IEC 27001:2013** A.16.1.6
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RS.IM-2: Response strategies are updated	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.RP-1: Recovery plan is executed during or after an event	· **CCS CSC** 8
	· **COBIT 5** DSS02.05, DSS03.04
	· **ISO/IEC 27001:2013** A.16.1.5
	· **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
RC.IM-1: Recovery plans incorporate lessons learned	· **COBIT 5** BAI05.07
	· **ISA 62443-2-1** 4.4.3.4
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.IM-2: Recovery strategies are updated	· **COBIT 5** BAI07.08
	· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RC.CO-1: Public relations are managed	· **COBIT 5** EDM03.02
RC.CO-2: Reputation after an event is repaired	· **COBIT 5** MEA03.02

Subcategory	Informative References from Cybersecurity Framework
RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	· **NIST SP 800-53 Rev. 4** CP-2, IR-4