Maritime Bulk Liquids Transfer,

Offshore Operations, and Passenger Vessel Cybersecurity Framework Profiles

December 2017

VERSION 3

This publication is available free of charge. More information on U.S. Coast Guard’s efforts in cybersecurity can be found <http://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/>.



Table of Contents

[Executive Summary v](#_Toc502846371)

[Background v](#_Toc502846372)

[The Profile vi](#_Toc502846373)

[Benefits vi](#_Toc502846374)

[1. Introduction 1](#_Toc502846375)

[1.1. Purpose 1](#_Toc502846376)

[1.2. Audience and How to Use this Document 1](#_Toc502846377)

[1.3. Document Structure 2](#_Toc502846378)

[1.4. Overview of the MBLT, Offshore Operations, and Passenger Vessel CFPs 2](#_Toc502846379)

[2. Background 6](#_Toc502846380)

[2.1. Cybersecurity and the Critical Infrastructure 6](#_Toc502846381)

[2.2. Cybersecurity Risk in the MBLT and Offshore Operations Enterprises 6](#_Toc502846382)

[2.2.1. Information Technology (IT) and Operational Technology (OT) 7](#_Toc502846383)

[2.2.2. IT Cybersecurity Risk 7](#_Toc502846384)

[2.2.3. OT Cybersecurity Risk 7](#_Toc502846385)

[2.3. Regulatory Context 8](#_Toc502846386)

[3. Using the Cybersecurity Framework 10](#_Toc502846387)

[3.1. Cybersecurity Framework Basic Elements 10](#_Toc502846388)

[3.2. Cybersecurity Framework Profiles 11](#_Toc502846389)

[3.3. Developing a Profile 13](#_Toc502846390)

[3.4. Advantages of Developing a Profile 14](#_Toc502846391)

[4. The MBLT, Offshore Operations, and Passenger Vessel CFPs for Industry 15](#_Toc502846392)

[4.1. Overall Process to Create this Profile 15](#_Toc502846393)

[4.2. Activities to Date 16](#_Toc502846394)

[4.3. Profile Foundations 17](#_Toc502846395)

[4.4. Governance 19](#_Toc502846396)

[5. Roadmap for Organizations Using the MBLT, Offshore Operations, and Passenger Vessel CFPs 20](#_Toc502846397)

[5.1. Profile Development and Use for MBLT and Offshore Operations Organizations 20](#_Toc502846398)

[5.2. Process to Incorporate the MBLT, Offshore Operations, and Passenger Vessel Profiles in Organizations 20](#_Toc502846399)

[6. Mission Mapping, Cybersecurity Framework Functions, Categories, and Subcategories 22](#_Toc502846400)

[6.1. MBLT Mission Objectives 23](#_Toc502846401)

[6.2. Summary of MBLT Priority Subcategories 26](#_Toc502846402)

[6.3. Offshore Operations Mission Objectives 37](#_Toc502846403)

[6.4. Summary of Offshore Operations Priority Subcategories 42](#_Toc502846404)

[6.5. Passenger Vessel Operations Mission Objectives 60](#_Toc502846405)

[6.6. Summary of Offshore Operations Priority Subcategories 63](#_Toc502846406)

[Appendix A. MBLT Profile A-1](#_Toc502846407)

[A-1 Mission Objective 1: Maintain Personnel Safety A-3](#_Toc502846408)

[A-2 Mission Objective 2: Maintain Environmental Safety A-14](#_Toc502846409)

[A-3 Mission Objective 3: Maintain Operational Security A-22](#_Toc502846410)

[A-4 Mission Objective 4: Maintain Preparedness A-41](#_Toc502846411)

[A-5 Mission Objective 5: Maintain Quality of Product A-55](#_Toc502846412)

[A-6 Mission Objective 6: Meet HR Requirements A-64](#_Toc502846413)

[A-7 Mission Objective 7: Pass Required Audits/Inspections A-75](#_Toc502846414)

[A-8 Mission Objective 8: Obtain Timely Vessel Clearance A-84](#_Toc502846415)

[Appendix B. Offshore Operations Profile B-1](#_Toc502846416)

[B-1 Mission Objective 1: Maintain Personnel Safety B-3](#_Toc502846417)

[B-2 Mission Objective 2: Maintain Environmental Safety B-27](#_Toc502846418)

[B-3 Mission Objective 3: Maintain Reliability B-53](#_Toc502846419)

[B-4 Mission Objective 4: Maintain Continuity and Integrity of Operations B-77](#_Toc502846420)

[B-5 Mission Objective 5: Maintain Cyber Situational Awareness B-98](#_Toc502846421)

[B-6 Mission Objective 6: Maintain Personnel Competencies B-115](#_Toc502846422)

[B-7 Mission Objective 7: Maintain Consistent and Effective Stakeholder Communications B-126](#_Toc502846423)

[B-8 Mission Objective 8: Maintain Operational Efficiency B-141](#_Toc502846424)

[B-9 Mission Objective 9: Maintain Secure Communications B-160](#_Toc502846425)

[B-10 Mission Objective 10: Maintain Regulatory Compliance/Compliance with Regulatory Audits & Inspection Requirements B-181](#_Toc502846426)

[B-11 Mission Objective 11: Maintain Third Party Integration B-196](#_Toc502846427)

[B-12 Mission Objective 12: Maintain Logistics B-214](#_Toc502846428)

[Appendix C. Passenger Vessel Operations Profile C-1](#_Toc502846429)

[C-1 Mission Objective 1: Maintain Human Safety C-3](#_Toc502846430)

[C-2 Mission Objective 2: Maintain Marine Safety and Resilience C-12](#_Toc502846431)

[C-3 Mission Objective 3: Maintain Environmental Safety C-23](#_Toc502846432)

[C-4 Mission Objective 4: Maintain Guest Support, Basic Hotel Services C-32](#_Toc502846433)

[C-5 Mission Objective 5: Maintain Regulatory Compliance C-45](#_Toc502846434)

[C-6 Mission Objective 6: Assure Secure Communications by Function and Mode C-56](#_Toc502846435)

[C-7 Mission Objective 7: Optimize and Enhance Guest Experience and Value C-72](#_Toc502846436)

[C-8 Mission Objective 8: Maintain Supply Chain and Turnaround C-83](#_Toc502846437)

[C-9 Mission Objective 9: Disembarking, Embarking, and Turnaround C-90](#_Toc502846438)

[C-10 Mission Objective 10: Coordinate Port Operations C-101](#_Toc502846439)

[C-11 Mission Objective 11: Assure (Optimize) Asset Lifecycle Management C-116](#_Toc502846440)

[C-12 Mission Objective 12: Maintain Passenger Information and Accounting Systems C-124](#_Toc502846441)

[C-13 Mission Objective 13: Manage, Monitor, and Maintain Non-Guest-Facing Back Office Technology C-136](#_Toc502846442)

[Appendix D. Industry Cybersecurity Processes & Profile Mappings D-1](#_Toc502846443)

[D-1 Energy Sector Cybersecurity Efforts and the DOE C2M2 Program D-1](#_Toc502846444)

[Energy Sector Cybersecurity D-1](#_Toc502846445)

[DOE Cybersecurity D-1](#_Toc502846446)

[D-2 Cybersecurity Framework Informative References D-4](#_Toc502846447)

[D-3 Mapping of Optional Resources D-4](#_Toc502846448)

List of Figures & Tables

[Figure 1‑1. Relationship Between Cybersecurity Framework and an Organization 1](#_Toc503256550)

[Figure 1‑2. Framework Core: Functions and Categories 3](#_Toc503256551)

[Figure 3‑1. Elements of the Cybersecurity Framework 10](#_Toc503256552)

[Figure 3‑2. Functions, Categories, and Subcategories of the Cybersecurity Framework 11](#_Toc503256553)

[Figure 3‑3. Mapping Mission Priorities 13](#_Toc503256554)

[Figure 4‑1. MBLT, Offshore Operations, and Passenger Vessel Operations CFPs Development Process 15](#_Toc503256555)

[Figure 5‑1. Steps to Applying Profiles to Your Organization 21](#_Toc503256556)

[Table 6‑1. MBLT Mission Objectives 24](#_Toc503256557)

[Table 6‑2. Summary of MBLT Subcategory Priorities by Mission Objective 26](#_Toc503256558)

[Table 6-3. Offshore Operations Mission Objectives 37](#_Toc503256559)

[Table 6‑4. Summary of Offshore Operations Subcategory Priorities by Mission Objective 42](#_Toc503256560)

[Table 6-5. Passenger Vessel Mission Objectives 60](#_Toc503256561)

[Table 6‑6. Summary of Offshore Operations Subcategory Priorities by Mission Objective 63](#_Toc503256562)

[Figure A‑1. Appendix A Content Legend A-2](#_Toc503256563)

[Figure B‑1. Appendix B Content Legend B-2](#_Toc503256564)

[Figure C‑1. Appendix C Content Legend C-2](#_Toc503256565)

[Table D‑1. Summary of Framework Use Steps D-2](#_Toc503256566)

# **Executive Summary**

White House Executive Order (EO) 13636tasked 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, Offshore Operations as its second Profile, and Passenger Vessel Operations as its third Profile. They are all presented in this integrated document. The CFPs identify and prioritize the minimum subset of Cybersecurity Framework Subcategories required to conduct operations in each context 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, Offshore, and Passenger Vessel operations have not always relied on combined Information Technology (IT) and Operational Technology (OT) processes, they are increasingly doing so. This introduces new cybersecurity risks that operators are working to manage.

Offshore Operations, both in drilling operations and in production operations, have evolved into complex and integrated systems, on and off facilities and vessels. Like MBLT, increased reliance on platform IT and OT as well as onshore connectivity has increased the potential attack surface against offshore operations.

Passenger Vessel Operations are also a complex and integrated mix of IT and OT Mission Objectives for both the ship operations aspect of the Profile and for the hotel operations aspect of the Profile. Like the MBLT and Offshore Operations Profiles, complex interactions are necessary for successful passenger vessel operations. Additionally, the hotel and entertainment operations on a modern passenger vessel present their own cybersecurity complexities.

Appropriate security controls must be in place to support the proper operation of organizational processes such as human resources, training, and business communication. Similarly, OT security controls for storage, 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, Offshore Operations, and Passenger Vessel Operations can only be appropriately managed through an integrated assessment, mitigation, and recovery strategy for both IT and OT systems. MBLT and Offshore Operations are 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 and Offshore Operations mission areas cover 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 broader enterprise risk management approach. Some of those risks arise from IT systems used to support OT systems. Likewise, Passenger Vessel Operations require participate in a complex worldwide supply chain of IT, OT, staffing, outsourcing, turnaround operations, and hotel and entertainment operations.

## **The Profile**

This CFP serves to assist in cybersecurity risk assessments for those entities involved in MBLT, Offshore Operations, and Passenger Vessel Operations as overseen by the USCG. It is intended to act as non-mandatory guidance to organizations conducting Passenger Vessel Operations, MBLT, Offshore Operations within facilities and vessels under the regulatory control of the USCG under the Code of Federal Regulations (CFR) 33 CFR 104, 143-147, and 154-156. This CFP serves to recommend cybersecurity safeguards and describes the desired minimum state of cybersecurity program for those organizations in each operational context.

The USCG consulted NIST regarding its work on the Cybersecurity Framework, and because of those discussions determined that industry-focused Cybersecurity Framework Profiles 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 joint mission areas of both USCG and industry.

During the development of these MBLT and Offshore Operations CFPs, the team engaged MBLT subject matter experts as well as experts in both the drilling and production phases of Offshore Operations. Likewise, during the development of the Passenger Vessel Profile, industry experts were consulted. Their collective expertise was used in identifying the sets of Mission Objectives and identifying the priority Cybersecurity Framework Categories and Subcategories for each Mission Objective for the MBLT, Offshore Operations, and Passenger Vessel Operations.

## **Benefits**

Creating industry-focused Cybersecurity Framework Profiles for MBLT, Offshore Operations, and Passenger Vessel Operations 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 each operational environment to allow for consistent analysis of cybersecurity-risk
* aligns industry and USCG cybersecurity priorities

These Profiles also enable strategic communications between:

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

# **Introduction**

## **Purpose**

These Maritime Bulk Liquids Transfer (MBLT), Offshore Operations, and Passenger Vessel Operations Cybersecurity Framework Profiles (CFPs) are industry-specific instantiations of the Cybersecurity Framework Profile concept for subsectors of the oil and natural gas industry (ONG) and Passenger Vessel industry.[[1]](#footnote-1) They are intended to act as non-mandatory guidance to organizations conducting Passenger Vessel Operations, MBLT and Offshore Operations within facilities and vessels under the regulatory control of the USCG under the Code of Federal Regulations (CFR) 33 CFR 104, 143-147, and 154-156. These CFPs recommend cybersecurity safeguards and describe the desired minimum state of cybersecurity for those organizations in the MBLT, Offshore Operations, and Passenger Vessel Operations contexts in support of those safety-oriented regulations. This guidance serves to assist in cybersecurity risk assessments for those entities involved in MBLT, Offshore Operations, and Passenger Vessel Operations as overseen by the USCG. The prioritized cybersecurity activities in the CFPs act as a starting point for enterprises to review and adapt their risk management processes due to increased awareness of cybersecurity threats in the relevant IT and OT environments. 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

## **Audience and How to Use this Document**

The MBLT, Offshore Operations, and Passenger Vessel CFPs are intended for use by executives, risk managers, cybersecurity professionals, vessel operators, and others with a role in cybersecurity risk management. This document should be used by those involved in overseeing, developing, implementing and managing the cybersecurity components of operations. Executive-level personnel should utilize the [Executive Summary](#_Executive_Summary), [Section 2](#_Background), and [Section 6](#_Mission_Mapping,_Cybersecurity), to gain an understanding of the purpose and scope of these MBLT and Offshore Operations CFPs. Managers should utilize all main chapters of the CFPs. Implementers should use the entire document including all appendices to understand the need for the CFPs and their specific contents.

## **Document Structure**

The remainder of this document is organized as follows:

* [Section 1](#_Introduction) provides an overview of Cybersecurity Framework Profiles and a description of the MBLT, Offshore Operations, and Passenger Vessel CFPs.
* [Section 2](#_Toc449104442) provides background information on Critical Infrastructure, the cybersecurity risk in the MBLT, Offshore Operations, and Passenger Vessel Operations enterprises, Information Technology (IT) and Operational Technology (OT), and the regulatory context.
* [Section 3](#_Using_the_Cybersecurity) discusses the Cybersecurity Framework and its components, including background about how Profiles emerge from it.
* [Section 4](#_The_MBLT_and) describes the approach used to create these Profiles, activities to date, and the foundations for the Profiles.
* [Section 5](#_Roadmap_for_Organizations) gives a roadmap for organizations that plan to use the MBLT, Offshore Operations, and Passenger Vessel Operations CFPs, and provides a process for organizations to incorporate these Profiles into cybersecurity risk management processes within their organization.
* [Section 6](#_Mission_Mapping,_Cybersecurity) identifies Mission Objectives and provides summary mappings to Cybersecurity Framework Functions, Categories, and Subcategories for the Profiles.
* Appendix A provides detailed Subcategory specifications for each MBLT Mission Objective.
* Appendix B provides detailed Subcategory specifications for each Offshore Operations Mission Objective.
* Appendix C provides detailed Subcategory specifications for each Passenger Vessel Mission Objective.
* Appendix D provides further resources regarding Cybersecurity Framework Profiles and assessment processes for other industries.

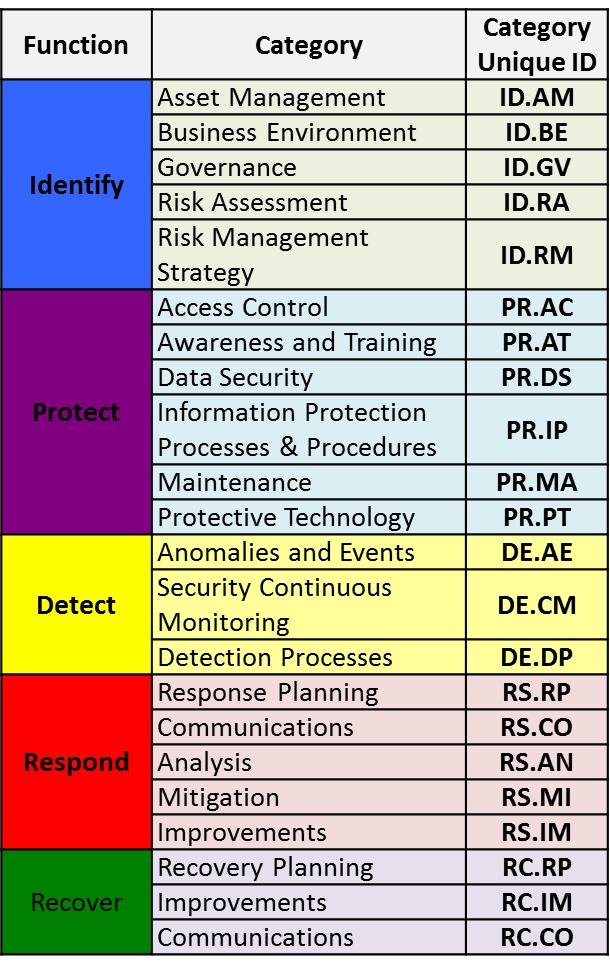
## **Overview of the MBLT, Offshore Operations, and Passenger Vessel CFPs**

The MBLT, Offshore Operations, and Passenger Vessel CFPs use 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]](#footnote-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.

Figure 1‑2. Framework Core: Functions and Categories



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, Offshore Operations and Passenger Vessel 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](#_MBLT_CFP_Structure). In order to help organizations prioritize and allocate resources most effectively, the Subcategories have been assigned priority levels that are described in [Section 6.2](#_Summary_of_MBLT). Appendix A provides the full detailed MBLT CFP.

Cybersecurity practices for Offshore Operations rely on the twelve Mission Objectives:

1. Maintain Personnel Safety
2. Maintain Environmental Safety
3. Maintain Reliability
4. Maintain Continuity and Integrity of Operations
5. Maintain Cyber Situational Awareness
6. Maintain Personnel Competencies
7. Maintain Consistent and Effective Stakeholder Communications
8. Maintain Operational Efficiency
9. Maintain Secure Communications
10. Maintain Regulatory Compliance/Compliance with Regulatory Audits and Inspections
11. Maintain Third Party Integration
12. Maintain Logistics

The Missions Objectives are defined in [Section 6.3](#_Offshore_Platform_Mission). In order to help organizations prioritize and allocate resources most effectively, the Subcategories have been assigned priority levels that are described in [Section 6.4](#_Summary_of_Offshore). Appendix B provides the full detailed Offshore Operations CFP.

Cybersecurity practices for Passenger Vessel Operations rely on the thirteen Mission Objectives:

1. Maintain Human Safety
2. Maintain Marine Safety and Resilience
3. Maintain Environmental Safety
4. Maintain Guest Support, Basic Hotel Services
5. Maintain Regulatory Compliance
6. Assure Secure Communications by Function and Mode
7. Optimize and Enhance Guest Experience and Value
8. Maintain Supply Chain and Turnaround
9. Disembarking, Embarking, and Turnaround
10. Coordinate Port Operations
11. Assure (Optimize) Lifecycle Asset Management
12. Maintain Passenger Information and Accounting Systems
13. Manage, Monitor, and Maintain Non-Guest-Facing Back Office Technology

The Missions Objectives are defined in Section 6.5. In order to help organizations prioritize and allocate resources most effectively, the Subcategories have been assigned priority levels that are described in Section 6.6. Appendix C provides the full detailed Passenger Vessel Operations CFP.

# **Background**

## **Cybersecurity and the Critical Infrastructure**

White House Executive Order (EO) 13636[[3]](#footnote-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]](#footnote-4), [[5]](#footnote-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 the 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]](#footnote-6) The five Functions are: Identify, Protect, Detect, Respond, and Recover. Each of the Functions are further divided into Categories and Subcategories.

## **Cybersecurity Risk in the MBLT and Offshore Operations Enterprises**

The Department of Homeland Security designated the Transportation Systems Sector, which includes the Maritime Transportation System, as one of the 16 critical infrastructure sectors to our nation.[[7]](#footnote-7) As defined by DHS, the Marine Transportation System consists of about 95,000 miles of coastline, 361 ports, more than 25,000 miles of waterways, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water. Parts of the Maritime Transportation System overlap with the Energy Sector, which is another of the 16 critical infrastructure sectors and includes both oil and natural gas as two of its three subsectors. MBLT, Offshore Operations, and Passenger Vessel Operations represent significant activities in these critical infrastructure sectors. The focus for the purposes of these USCG Profiles is to address the Marine Transportation System.

## **Information Technology (IT) and Operational Technology (OT)**

Although MBLT, Offshore Operations, and Passenger Vessel Operations have not always relied as heavily on combined IT and OT processes, they are increasingly doing so. This introduces new cybersecurity risks that MBLT, Offshore Operations, and Passenger Vessel 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. 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 of the storage, transfer, pressure monitoring, vapor monitoring, emergency response, and spill mitigation systems to meet human safety and environmental safety needs. 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, Offshore Operations, and Passenger Vessel Operations can be appropriately managed as part of an integrated risk management system.

MBLT and Offshore Operations are 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 and Offshore Operations mission areas cover a blend of enterprise IT and OT. Likewise, Passenger Vessel Operations depend on both enterprise IT and OT to operate seamlessly. 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.

## **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 corporate 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.

## **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, Offshore Operations, and Passenger Vessel Operations are supported by OT as they protect human and environmental safety.

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 efficiencies to 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]](#footnote-8) Exchange and validation of information about threats is supported by the ICS Cyber Emergency Response Team (ICS‑CERT)[[9]](#footnote-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]](#footnote-10) and conducts assessments[[11]](#footnote-11).

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

## **Regulatory Context**

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

* Outer Continental Shelf Activities 33 CFR Subchapter N
* facilities transferring oil or hazardous material in bulk (33 CFR 154)
* maritime security for vessels (33 CFR 104)
* oil or hazardous material pollution prevention regulations for vessels (33 CFR 155)
* oil and hazardous material transfer operations (33 CFR 156)

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[[12]](#footnote-12)
* cybersecurity-related interviews with several of its Federal Advisory Committees[[13]](#footnote-13), [[14]](#footnote-14) concerned with safety 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 industry-focused Cybersecurity Framework Profiles should be created. NIST personnel who oversaw the development of the Cybersecurity Framework along with personnel from its NCCoE [[15]](#footnote-15) 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.

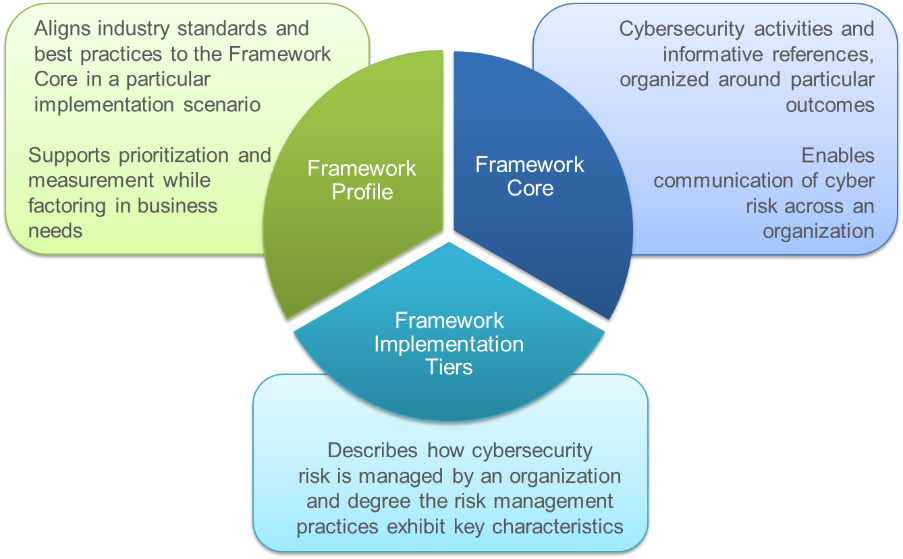
The USCG is working with industry to develop these voluntary industry-focused Profiles to mitigate risks in their joint mission areas. The USCG determined the first industry-focused Profile should address MBLT, the second should address Offshore Operations, and the third should address Passenger Vessel Operations.

# **Using the Cybersecurity Framework**

## **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

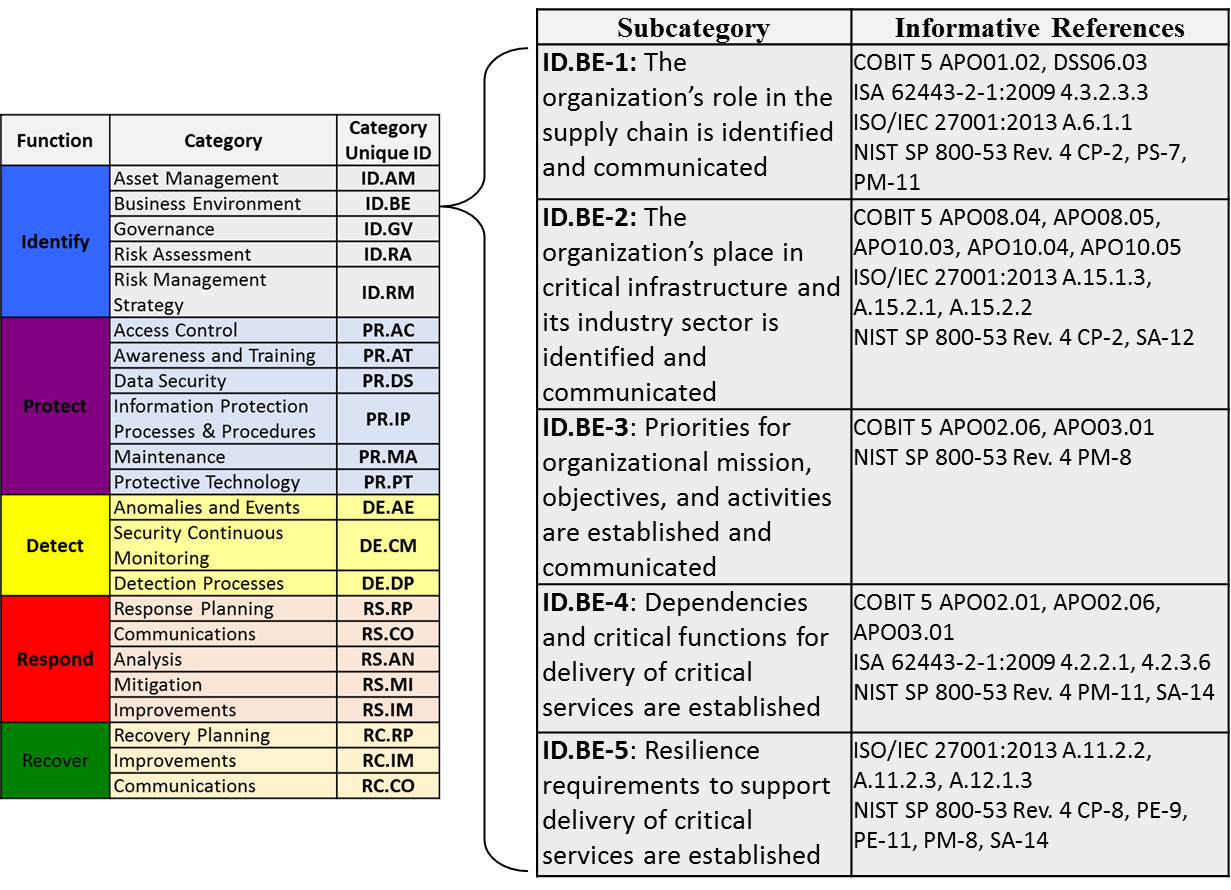


The Framework Core is structured into five Functions that identify the key cybersecurity outcomes identified to manage cybersecurity risk:

* **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



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?

## **Cybersecurity Framework Profiles**

#### Overview of Profiles

As organizations determines how to use the Cybersecurity Framework Core to assist in managing their cybersecurity risks, they can develop organization-specific Profiles to map their current state and a desired future state based on their 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 operational environment
* align industry and USCG cybersecurity priorities

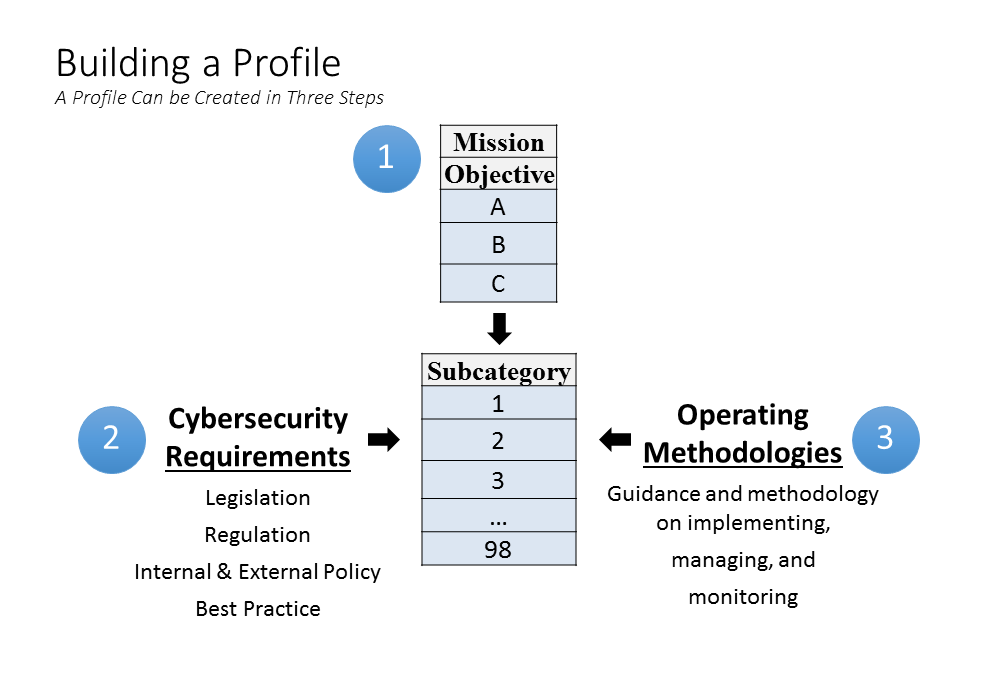
Organizations that are part of an industry or sub-sector that has one or more industry-focused Profiles generally use those industry-focused Profiles to inform decisions made when constructing their organization-focused Profiles and measuring progress.

## **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 does 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?

Organizations 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 an organization reviews operating methodologies[[16]](#footnote-16), 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.

## **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 methodologies is less intrusive to ongoing operations
* identifying cybersecurity gaps regarding technology, processes, and people

Each organization implementing these Profiles has the ability to map its current capabilities to the MBLT and/or Offshore Operations CFP. This can support a gap analysis to assist organizations in attaining the desired state of full implementation of the CFPs. Further, the MBLT, Offshore Operations, and Passenger Vessel Operations CFPs can be tailored organizations to identify an organizationally-specific desired ‘to be’ state. This process allows organizations to use the gap analysis to drive budget, schedules, and resource allocations as they plan for achieving their desired state. These Profiles are 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.

# **The MBLT, Offshore Operations, and Passenger Vessel CFPs for Industry**

While [Section 3](#_Using_the_Cybersecurity) discusses Cybersecurity Framework Profiles generally, this section discusses the process to create and implement industry-specific MBLT, Offshore Operations, and Passenger Vessel CFPs to add a cybersecurity dimension to existing risk management plans. This section describes the steps in the Profile development process, the regulatory and statutory foundations for the CFPs, and governance.

## **Overall Process to Create this Profile**

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

Figure 4‑1. MBLT, Offshore Operations, and Passenger Vessel Operations CFPs Development Process

#### Plan

The Plan phase involved the development of an awareness of the regulatory framework surrounding MBLT, Offshore Operations, and Passenger Vessel Operations. The existing regulatory framework is ambiguous regarding cybersecurity in MBLT, Offshore Operations, and Passenger Vessel Operations. However, MBLT, Offshore Operations, and Passenger Vessel 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 International Association of Drilling Contractors (IADC), the Offshore Operators Committee (OOC), the Passenger Vessel Association (PVA), the Cruise Line Industry Association (CLIA), and attendance at industry conferences. A series of in‑person discussion sessions were held with stakeholders to develop the Mission Objectives defined in [Section 6.1](#_MBLT_CFP_Structure) , [6.3](#_Offshore_Platform_Mission) and 6.5 to identify the priority Categories 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 operational environments. Through these steps, 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 revisions incorporated in response to industry feedback. The MBLT, Offshore Operations and Passenger Vessel Profiles were further developed by identifying and prioritizing the Cybersecurity Framework Subcategories in support of each Mission Objective. Initial work products were shared with industry contributors that participated in the Scope phase to elicit feedback. For the MBLT CFP, an initial working version was shared with 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. For the Offshore Operations Profile, meetings were held with IADC, API, and the OOC. Additionally, a “content preview” was published on the USCG Maritime Commons blog in June 2017. For the Passenger Vessel Profile, preparatory and in-person meetings were held with the PVA and CLIA and a Passenger Vessel content preview was shared as well.

#### Publish

In the Publish phase, the USCG releases the Profiles to the broader maritime community. They are then available for organizations involved in MBLT, Offshore Operations, and Passenger Vessel Operations to incorporate into their enterprise risk management processes.

#### Maintain

In the Maintain phase, the Profiles will be monitored for usefulness. Any gaps will be identified and recorded. Over time, updates to the Profiles 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, Offshore Operations, and Passenger Vessel regulations. As regulation, policy, and technical capabilities change, these Profiles will need to be reviewed and possibly revised under whatever governance process is ultimately determined.

## **Activities to Date**

For the MBLT operations 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 Categories 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 the initial version of this document. As part of this process, the NCCoE delivered that initial version to the USCG for industry use.

A similar process was followed for the Offshore Operations CFP. A series of workshops was held in Houston during early 2017 to refine the scope of the Profile, validate Mission Objectives, and prioritize Cybersecurity Framework Categories. This included sessions with the IADC, API, and the OOC. The USCG and NCCoE then mapped Cybersecurity Framework Subcategories to each Mission Objectives, based on prioritized Cybersecurity Framework Categories, and continued interactions with trade associations and industry subject matter experts during the Draft phase. This document was expanded to add the Offshore Operations CFP content, and NCCoE delivered this updated version to the USCG for industry use.

Likewise, a similar process was followed for the Passenger Vessel Profile. A workshop was held in Ft. Lauderdale in late April 2017. Following the workshop, the USCG shared initial results with the PVA and CLIA.

## **Profile Foundations**

The following authorities and resources form the basis for the MBLT and Offshore Operations CFPs:

* 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 11/3/17]
* United States Coast Guard (USCG) and Code of Federal Regulations (CFR) (33 CFR 104, 143-147 and 154-156) requirements, [http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title33/33cfr154\_main\_02.tpl](http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title33/33cfr154_main_02.tpl%20) [accessed 11/3/17]
* 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 11/3/17]
* 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 11/3/17]
* 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 11/3/17]
* Executive Order no. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017 (The White House) <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal> [accessed 11/3/17]
* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014. <https://www.nist.gov/cyberframework> [accessed 11/3/17]
* Cybersecurity Capability Maturity Model, v 1.1, February 2014. <http://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program> [accessed 11/3/17]

Additionally, the U.S. maritime and ONG industry uses 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 Bureau of Shipping, Rules for Building and Classing Mobile Offshore Drilling Units, 2017, <https://ww2.eagle.org/en/rules-and-resources/rules-and-guides.html#/content/dam/eagle/rules-and-guides/current/offshore/6_rules_building_classing_mobile_offshore_drilling_units> [accessed 11/3/17].
* 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.*[[17]](#footnote-17)
* 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 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 Publication800-53, 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 11/3/17]
* North American Electric Reliability Council (NERC), Critical Infrastructure Protection (CIP) Version 5.[[18]](#footnote-18)
* 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 11/3/17].

## **Governance**

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

# **Roadmap for Organizations Using the MBLT, Offshore Operations, and Passenger Vessel CFPs**

The MBLT, Offshore Operations, and Passenger Vessel CFPs are 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.

## **Profile Development and Use for MBLT and Offshore Operations Organizations**

The Cybersecurity Framework describes a seven-step process for organizations to use the Cybersecurity Framework for planning and risk mitigation when creating or improving cybersecurity programs.[[19]](#footnote-19) 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 Profiles for MBLT, Offshore Operations, and Passenger Vessel Operations per Step 3. These Profiles provide an industry view of cybersecurity priorities for the MBLT and Offshore Operations subsectors of the ONG industry as well as for the Passenger Vessel industry. Organizations may use these Profiles 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. These Profiles act 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 Target Profile to perform Steps 6 and 7 to address its specific priorities.

## **Process to Incorporate the MBLT, Offshore Operations, and Passenger Vessel Profiles in Organizations**

As an organization utilizes these Profiles and complete the steps outlined above, it should fold its implementation of the Profiles into its enterprise. Each organization, with its understanding of policy drivers, relevant standards, and other Cybersecurity Framework Profiles, should adapt these Profiles to meet its needs regarding compliance with regulations and best practices for MBLT, Offshore Operations, and Passenger Vessel 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, Offshore Operations, and Passenger Vessel Operations Profiles and incorporate them into its 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 an 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, an organization can assess where it is against where it would like to be, using the inputs identified in the previous step (e.g., the MBLT, Offshore Operations, and Passenger Vessel Operations Profiles). The outcomes of the assessment inform the next step, developing the strategy and specific plans for implementing the Profiles (and other cybersecurity initiatives identified) within an organization. **Making the necessary changes within an organization occurs during the incorporate phase.**

Figure 5‑1. **Steps to** Applying Profiles to Your Organization

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

# **Mission Mapping, Cybersecurity Framework Functions, Categories, and Subcategories**

The MBLT, Offshore Operations, and Passenger Vessel Profiles are customizations of the Cybersecurity Framework for industry subsectors based on input from subject matter experts on existing processes, cybersecurity capabilities and operational technology. The CFPs fuse business and mission logic in the implementation of USCG regulations. They align cybersecurity with operational methods. As they are utilized by organizations, the CFPs can supplement their existing cybersecurity risk management processes.

The MBLT, Offshore Operations, and Passenger Vessel CFPs use 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. The MBLT, Offshore Operations, and Passenger Vessel Operations CFPs each have a set of Mission Objectives tailored to their operating context.

Organizations should strive to conduct activities in support of all relevant Subcategories in the Cybersecurity Framework. The MBLT, Offshore Operations, and Passenger Vessel CFPs recognize that expectation and further specify 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 the CFPs as input into future prioritization and improvement activities. Subcategory selections are included for each of the Mission Objectives required to conduct operations in a more secure manner within the context of each CFP.

From the perspective of the USCG and industry participants that contributed to development of these Profiles, 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 these CFPs[[20]](#footnote-20):

* **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, 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.

Risk management programs and cybersecurity decisions vary in accordance with the unique needs of each organization. Priorities, emphasis, and approaches to addressing Subcategories may differ from organization to organization. For that reason, the CFPs do 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.

## **MBLT Mission Objectives**

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 Table 6-1.

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 |
| **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   + risk mitigation procedures   + ongoing situational awareness   + backup/resilience/fail-safe modes   + 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:   + testing   + preventive maintenance   + remediation   + ongoing situational awareness * manage prominent and increasing role of automated systems in maintaining control of product during safe transport. |
| **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:   + 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 |
| **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](#_Summary_of_MBLT) 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](#_Summary_of_MBLT), 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.

## **Summary of MBLT Priority Subcategories**

Table 6-2 provides a summary of Subcategory priorities by Mission Objective. This is further defined in Appendix A, which provides the full detailed MBLT CFP.

Table 6‑2. Summary of MBLT 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 and the organization’s risk strategy. | **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 |  |  |  |  |  |  |  |  |
| **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., deprovisioning, personnel screening) |  |  |  |  |  |  |  |  |
| **PR.IP-12:** Avulnerability 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 ismonitored 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:** Responseplans 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 |  |  |  |  |  |  |  |  |

## **Offshore Operations Mission Objectives**

In order to align the Cybersecurity Framework with the mission needs of Offshore 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 Offshore Operations rely on the twelve Mission Objectives defined in Table 6-3.

Table 6-3. Offshore Operations Mission Objectives

| **Mission Objective** | **Description** |
| --- | --- |
| **1: Maintain Personnel Safety** | Recognizing cybersecurity-effects on process control systems that impact personnel safety. Preventing injury, including loss of life through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, Recovery Planning, and Recovery Communications. Organizations should:   * account for all personnel on board offshore facilities and vessels * understand scope of operational threats and their potential adverse impacts to people * manage risks to personnel using a structured process * identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact personnel safety * implement Detect/Respond/Recover activities where cybersecurity adversely affects personnel safety |
| **2: Maintain Environmental Safety** | Recognizing cybersecurity-effects on process control systems that impact environmental safety. Preventing harm to the environments and ecosystems through: Asset Management, Risk Assessment, Access Control, Awareness and Training, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes, Response Planning, Response Communications, Recovery Planning, and Recovery Communications. Organizations should:   * account for all processes that may affect the environment * understand scope of operational threats and their potential adverse impacts to the environment * manage risks to the environment using a structured process * identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact environmental safety * manage prominent and increasing role of automated systems in maintaining offshore operations * implement Detect/Respond/Recover (e.g., respond and remediate) activities where cybersecurity adversely affects environmental safety |
| **3: Maintain Reliability** | Preserving systems integrity so that they function as designed and intended throughout their planned life. Prevention of accidents and adverse business impacts through: Risk Assessment; Anomaly Detection; Asset Management; and Protective Technology. Organizations should:   * manage risks to reliability using a structured process * examine components that can cause failure alone or in combination * design IT and OT integration points to fail safely within the system’s operational environment * preserve a steady state of containment when not in operation |
| **4: Maintain Continuity and Integrity of Operations** | Preserving the ability to operate at the intended level within the desired time frame. System functions without interruption through: Asset Management, Risk Assessment, Access Control, Information Protection Processes and Procedures, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring. Organizations should:   * incorporate outcomes of risk assessments into facility and organizational management systems as well as the systems engineering lifecycle and change management procedures * perform preventative maintenance * plan for backups and work arounds * implement redundancy for critical processes and assets * employ management of change procedures |
| **5: Maintain Cyber Situational Awareness** | Understanding and assessing cyber threats and vulnerabilities and the operational risks to which they can lead. System parameters are maintained within operational norms through: Risk Assessment, Awareness and Training, Information Protection Processes and Procedures, Protective Technology, Anomalies and Events, Security Continuous Monitoring, and Detection Processes. Organizations should:   * employ appropriate administrative, technical, and physical controls to protect IT and OT capabilities from potential adverse cyber-effects * monitor changes to technologies in use (e.g., vendor updates to software) * engage with communities that promote awareness of industry-specific threats and vulnerabilities (e.g., InfraGard, information sharing and analysis organizations that support the organization’s industry and or geographical locations) * provide adequate cybersecurity training to personnel, based on their role(s) |
| **6: Maintain Personnel Competencies** | Ensuring employees have adequate knowledge, skills, and abilities to support operations. Preventing personnel-based cyber incidents which may cause adverse cyber or physical effects through: Asset Management, Business Environment, Governance, Awareness and Training, Information Protection Processes and Procedures, and Communications. Organizations should:   * understand how personnel encounters with assets can result in cyber-causes with cyber or physical effects * identify and train personnel on interdependence of cybersecurity with operational responsibilities * employ contract resources for specializations that are not available within the organization * implement operational procedures that limit the possibility of human error where possible |
| **7: Maintain Consistent and Effective Stakeholder Communications** | Ensuring critical stakeholders are aware of operational environment. Supporting reliable and valuable communication with the right stakeholders at the right time through: Business Environment, Governance, Risk Management Strategy, Access Control, Information Protection Processes and Procedures, and Communications. Organizations should:   * identify stakeholders and establish all critical communication paths * manage reputation through clear, consistent messaging * implement communications procedures for supply chain partners and external entities related to response and recovery efforts when issues arise |
| **8: Maintain Operational Efficiency** | Ensuring offshore facility and vessel operations continue to function optimally. Promoting operational capabilities through: Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, Access Control, Data Security, Information Protection Processes and Procedures, Maintenance, and Improvements. Organizations should maintain standards that support tuning equipment for optimal performance. Organizations should:   * identify and manage assets and their relationships to business processes * identify and manage stakeholder roles, including third party roles, in efficient execution of business processes * protect business process integrity |
| **9: Maintain Secure Communications** | Ensuring communications required to operate positioning equipment and external communications are available reliably. Protecting communications channels through: Asset Management, Risk Assessment, Access Control, Data Security, Information Protection Processes and Procedures, Protective Technology, Anomalies and Events, Security Continuous Monitoring, and Detection Processes. Organizations should:   * understand the facility’s or vessel’s external communication paths * protect integrity of positioning equipment and other equipment that can be adversely impacted via external communication paths * protect personal information * implement redundant systems, where appropriate, to limit the risk of communications loss |
| **10: Maintain Regulatory Compliance/Compliance with Regulatory Audits & Inspection Requirements** | Ensuring compliance with regulations that would impact ability of operations to proceed. Sustaining acceptable levels of operational capabilities through: Business Environment, Governance, Risk Management Strategy, Awareness and Training, Information Protection Processes and Procedures, Maintenance, and Security Continuous Monitoring. Organizations should:   * track regulatory activity and assess impacts to operations * incorporate activities to address regulation changes into strategic plans, policies, processes, and procedures as well as facility and organizational management systems * develop on-going relationships with regulators * ensure foundational “cyber hygiene” activities are addressed as part of the overall risk management program * contribute to industry standards and best practices |
| **11: Maintain Third Party Integration** | Protecting the supply chain and operating seamlessly in a multi-party environment, through: Asset Management, Business Environment, Governance, Risk Assessment, Access Control, and Awareness and Training. Organizations should:   * manage relationships with suppliers, vendors, contractors, consultants, and other entities that support operational and business activities * communicate requirements and assess their implementation throughout the supply chain * understand the interplay between personnel from all entities involved in operations |
| **12: Maintain Logistics** | Managing the movement of personnel, equipment, and supplies that sustain operations, through: Asset Management, Business Environment, Risk Assessment, Risk Management Strategy, and Data Security. Organizations should:   * know which personnel should be where and when, and whether personnel are at the proper location as expected (e.g., the right person is on the right facility or vessel at the right time) * know which transportation modalities are in operation and where they are located (e.g., boats, helicopters) * protect the physical security of personnel, equipment, and supplies from the point of origin to destination * ensure supplies that support operations are available when needed (e.g., personnel supplies, such as food, and operational supplies, such as spare parts and back up equipment) |

## 

## **Summary of Offshore Operations Priority Subcategories**

Organizations should strive to conduct activities in support of all relevant Subcategories in the Cybersecurity Framework. The Offshore Operations 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 Offshore Operations CFP as input into future prioritization and improvement activities. Subcategory selections are included for each of the twelve Mission Objectives required to conduct Offshore Operations in a more secure manner.

Table 6‑4. Summary of Offshore Operations Subcategory Priorities by Mission Objective

| **Function** | **Category** | **Subcategory** | **Mission Objectives**   **= High Priority,**  **= Moderate Priority,**  **= Other Implemented Subcategories**  **🗙 = Subcategories to NOT Implement** | | | | | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **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 and the organization’s risk strategy. | **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 |  |  |  |  |  |  |  |  |  |  |  |  |
| **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 |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **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., deprovisioning, personnel screening) |  |  |  |  |  |  |  |  |  |  |  |  |
| **PR.IP-12:** Avulnerability 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 ismonitored 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:** Responseplans 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 |  |  |  |  |  |  |  |  |  |  |  |  |

## **Passenger Vessel Operations Mission Objectives**

In order to align the Cybersecurity Framework with the mission needs of Passenger Vessel 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 Passenger Vessel Operations rely on the thirteen Mission Objectives defined in Table 6-5.

Table 6-5. Passenger Vessel Mission Objectives

|  |  |  |
| --- | --- | --- |
| Mission Objective | | Description |
| 1. Maintain Human Safety | Recognizing cybersecurity-effects on process control systems that impact personnel safety. Preventing injury, including loss of life through: Risk Assessment, Awareness and Training, Maintenance, Protective Technology, and Response Planning. Organizations should:  • account for all personnel on board active equipment  • understand scope of operational threats and their impacts to people  • manage risks to personnel using a structured process  • identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact personnel safety  • implement Detect/Respond/Recover activities where cybersecurity adversely affects personnel safety | |
| 2.Maintain Marine Safety and Resilience | Preserving systems integrity so that they function as designed and intended throughout their planned life helps maintain marine safety and resilience. Prevention of accidents and business impacts through: risk assessment; anomaly detection; asset management; and protective technology. Organizations should:  • examine components that can cause failure alone or in combination  • design IT and OT integration points to "fail safe"  • preserve a steady state of containment when not in operation | |
| 3.Maintain Environmental Safety | Recognizing cybersecurity-effects on process control systems that impact environmental safety. Preventing harm to the environments and ecosystems through: Goverrnance, Risk Assessment, Awareness and Training, and Response Planning. Organizations should:  • account for all processes that may affect the environment  • understand scope of operational threats and their impacts to the environment  • manage risks to the environment using a structured process  • identify and train personnel on interdependence of cybersecurity with operational responsibilities that impact environmental safety  • manage prominent and increasing role of automated systems in maintaining operations  • implement Detect/Respond/Recover (e.g., respond and remediate) activities where cybersecurity adversely affects environmental safety | |
| 4.Maintain Guest Support, Basic Hotel Services | Recognize cybersecurity-effects on the guest support and hotel services aspect of a passenger vessel. Prevent harm to customers, the systems they use, employees, and services infrastructure such as booking, excursions, dining, entertainment, room service, and additional amenities:   * manage risk to all guest facing systems * maintain account management security * manage support systems security * identify and securely protect guest personally Identifiable Information (PII) * control interfaces and data shared with business partners for ship entertainment, excursion, and hotel services | |
| 5.Maintain Regulatory Compliance | Ensuring compliance with regulations that would impact ability of operations to proceed. Sustaining acceptable levels of operational capabilities through: Asset Management, Governance, Risk Management, and Awareness and Training. Organizations should:  • track regulatory activity and assess impacts to operations  • incorporate activities to address regulation changes into strategic plans, policies, processes, and procedures  • develop on-going relationships with regulators  • ensure foundational “cyber hygiene” activities are addressed as part of the overall risk management program  • contribute to industry standards and best practices | |
| 6.Assure Secure Communications by Function and Mode | Ensuring communications required to operate positioning equipment and ship-to-shore communications are available reliably. Protecting communications channels through: Risk Assessment, Data Security, Information Protection Processes and Procedures, Protective Technology, Anomalies and Event detection, and Security Continuous Monitoring. Organizations should:  • understand communication flows between ship and shore  • protect integrity of positioning equipment and other equipment that can be affected remotely  • protect personal information | |
| 7.Optimize and Enhance Guest Experience and Value | Recognize cybersecurity role in the guest experience. Prevent harm to customers in booking, excursions, dining, entertainment, room service, and additional amenities:   * provide seamless interface to guests as they request services * manage support systems security * identify and securely protect guest personally Identifiable Information (PII) * manage interfaces and data shared with business partners for ship entertainment, excursion, and hotel services | |
| 8.Maintain Supply Chain and Turnaround | Managing the movement of personnel, equipment, and supplies that sustain operations, though: Asset Management, and Risk Management Strategy. Organizations should:   * know which personnel should be where and when, and whether personnel are at the proper location as expected * protect the physical security of personnel, equipment, and supplies from the point of origin to destination * ensure supplies that support operations are available when needed | |
| 9.Disembarking, Embarking, and Turnaround | Manage the people aspect of port turnaround operations:   * coordinate departure of guests and coordination of their onward journey * coordination of transfer of guest luggage and other items between systems * coordinate arrival of guest and coordination with their mode of arrival * manage interfaces with all communications with shore and partner systems to provide seamless disembarking and embarking | |
| 10.Coordinate Port Operations | Manage the ship and supply coordination of Port Operations:   * coordination of port arrival and departure regulations, procedures, and protocols * coordination of incoming food and other perishable supplies * coordination of resupply of fuel * coordination of sewage offload | |
| 11.Assure(Optimize)  Lifecycle Asset Management | Manage and optimize the operational uptime of all capabilities:   * coordinate maintenance and repair to minimize disruption * assure ready spares and systems/process redundancy to assure availability * manage assets to track effective useable life, end of life swap out, systems replacement and upgrades | |
| 12. Maintain Passenger Information and Accounting Systems | Recognize cybersecurity role in the passenger back office systems:   * provide security to non-customer-facing IT * manage support systems security * identify and securely protect guest personally identifiable information (PII) * manage interfaces and data shared with business partners | |
| 13. Manage, Monitor and Maintain Non-Guest-Facing Back Office Technology | Recognize cybersecurity effects on the back-office operations. Prevent harm to systems and services infrastructure:   * manage risk to all back-office systems * maintain account management security * manage support systems security * identify and securely protect guest personally identifiable information (PII) * control interfaces and data shared with business partners | |

## **Summary of Offshore Operations Priority Subcategories**

Organizations should strive to conduct activities in support of all relevant Subcategories in the Cybersecurity Framework. The Passenger Vessel Operations 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 Passenger Vessel Operations CFP as input into future prioritization and improvement activities. Subcategory selections are included for each of the thirteen Mission Objectives required to conduct Passenger Vessel Operations in a more secure manner.

Table 6‑6. Summary of Offshore Operations 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** | **9** | **10** | **11** | **12** | **13** |
| **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 and the organization’s risk strategy. | **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 |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **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., deprovisioning, personnel screening) |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **PR.IP-12:** Avulnerability 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 ismonitored 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:** Responseplans 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 |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. As described in Section 1.1 of the Cybersecurity Framework, “A Framework Profile (“Profile”) represents the outcomes based on business needs that the 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).” [↑](#footnote-ref-1)
2. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, available at: <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf> (last visited November 3, 2017). [↑](#footnote-ref-2)
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> [↑](#footnote-ref-3)
4. <http://www.nist.gov/cyberframework/> [↑](#footnote-ref-4)
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> [↑](#footnote-ref-5)
6. Cybersecurity Framework, p. 4 [↑](#footnote-ref-6)
7. <https://www.dhs.gov/critical-infrastructure-sectors> [↑](#footnote-ref-7)
8. Department of Energy, National SCADA Test Bed, <http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity/national-scada-test-bed> [↑](#footnote-ref-8)
9. Department of Homeland Security, DHS, Industrial Control Systems Cyber Emergency Response Team, <https://ics-cert.us-cert.gov/> [↑](#footnote-ref-9)
10. DHS, ICS-CERT Standards and References, <https://ics-cert.us-cert.gov/Standards-and-References> [↑](#footnote-ref-10)
11. DHS, ICS-CERT Assessments, <https://ics-cert.us-cert.gov/Assessments> [↑](#footnote-ref-11)
12. *United States Coast Guard Cyber Strategy*, June 2015, <https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf> [↑](#footnote-ref-12)
13. 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> [↑](#footnote-ref-13)
14. 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> [↑](#footnote-ref-14)
15. National Cybersecurity Center of Excellence, <https://nccoe.nist.gov/> [↑](#footnote-ref-15)
16. [↑](#footnote-ref-16)
17. <https://www.cisecurity.org/critical-controls/> [↑](#footnote-ref-17)
18. 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> [↑](#footnote-ref-18)
19. 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). [↑](#footnote-ref-19)
20. The prioritization of Subcategories may vary between Profiles for ONG and other industries, and even subsectors within ONG, depending on Mission Objectives and other relevant factors to other Profiles. [↑](#footnote-ref-20)