Pacific Northwest
NATIONAL LABORATORY

PNNL-30256

# Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems

Revision 0

September 2020

Fleurdeliza A de Peralta
Mark D Watson
Ryan M Bays
Ford E Powers
Joshua R Boles

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
*operated by*
BATTELLE
*for the*
UNITED STATES DEPARTMENT OF ENERGY
*under Contract DE-AC05-76RL01830*

**Printed in the United States of America**

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov**

PNNL-30256

# Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems

Revision 0

September 2020

Fleurdeliza A de Peralta
Mark D Watson
Ryan M Bays
Ford E Powers
Joshua R Boles

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

# Abstract

The marine renewable energy (MRE) industry is an emerging source of power for marine applications, marine devices, and coastal communities. Developers of MRE systems rely on industrial control systems and information technology to support operations and maintenance activities. The advanced operational and information technology devices used in MRE systems create a pathway for a cyber-threat actor to gain unauthorized access to data or disrupt operation. To improve the resilience of MRE systems as predictable, affordable, and reliable sources of energy, the U.S. Department of Energy's Water Power Technologies Office funded Pacific Northwest National Laboratory to develop a guidance document that will assist MRE developers and end users with integrating security and safety into the operational and enterprise networks of MRE systems. The cybersecurity guidance document was developed by assessing cyber threats and consequences of a cyberattack on typical MRE system assets (Focus 1) and identifying industry best practices to protect the MRE system and end user from those threats (Focus 2). The results of Focus 1 are documented in a supplement report, PNNL-29802, *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems.* This report provides the results of Focus 2 and describes cybersecurity best practices commensurate with the risk of affecting the business and mission objectives of the end user. The cybersecurity best practices implement the core functions of the National Institute of Science and Technology Cybersecurity Framework (e.g., identify, detect, protect, respond, and recover). The methods to protect MRE systems are based on recommended strategies to mitigate known threats to the energy sector and security measures to protect information technology and industrial control systems. The cybersecurity best practices were tailored to protect information and operational technology assets expected on MRE systems and their end use from a cyberattack.  The best practices developed in this report are based on insights from security measures included in National Institute of Science and Technology guidance documents and other cybersecurity guidance documents developed for the maritime industry and energy industry (generation and distribution).

# Summary

Marine renewable energy (MRE) is a form of electrical power that is harnessed from the marine and riverine environment, including ocean tides, waves, currents, salinity gradients, temperature gradients, and riverine flows. The operational and information technology used in MRE system designs provides a cyberattack surface to gain unauthorized access to data or disrupt operation of the energy-generating device. The U.S. Department of Energy is committed to advancing electric power infrastructure security and, as a part of this, focusing on cybersecurity of energy-generating assets. Thus, the Water Power Technologies Office, within the Office of Energy Efficiency and Renewable Energy, has funded Pacific Northwest National Laboratory to address two focus areas:

1. Development of a framework for determining cybersecurity risks based on the potential cyber threats, likelihood of vulnerabilities, and consequences of a cyberattack on MRE systems.
2. Development of a cybersecurity guidance document that MRE stakeholders can use to mitigate cybersecurity risks.

The first focus area was addressed in the Pacific Northwest National Laboratory Report PNNL-29802, *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems* [1], which describes a graded approach to determine the risks based on a qualitative assessment of the likelihood of cybersecurity threats and the impact a cyberattack would have on the MRE system and the end user.

This report addresses the second focus area, which describes the MRE system risk management framework and identifies methods tailored to protect MRE systems commensurate with the risk from a cyberattack. The security measures follow the core functions described in the National Institute of Standards and Technology Cybersecurity Framework (e.g., identify, protect, detect, respond, and recover) and insights from industry documents developed to secure information systems and industrial control systems [8]. The cybersecurity best practices are grouped into nine categories:

- Account and Access Management
- Asset Management
- Communications Management
- Incident Preparedness
- Network Architecture and Security
- Physical and Environment Security
- Cybersecurity Program Management
- Cybersecurity Risk Management
- Security Development Practices

The eighty-six security measures identified in this report are based on initial insights from industry documents that protect industrial control systems, energy delivery systems, and the maritime industry. This report is an initial draft of cybersecurity best practices and will be updated as more information is available on MRE system designs and deployment configurations.

# Acknowledgments

This document was prepared by Pacific Northwest National Laboratory for the U.S. Department of Energy's Water Power Technologies Office within the Office of Energy Efficiency and Renewable Energy. Special thank you is extended to Dr. Mark Christian of the Water Power Technologies Office for his dedication and leadership in developing this document. Special thank you is also extended to the various stakeholders in the marine renewable energy industry for providing insights to the Pacific Northwest National Laboratory team on the technology and operational configurations of their designs and expected applications.

# Acronyms and Abbreviations

| | |
|---|---|
| ABS | American Bureau of Shipping |
| AC | Account and Access (Management) |
| AM | Asset Management |
| ATT&CK$^{TM}$ | Adversarial Tactics, Techniques and Common Knowledge |
| BES | bulk electrical system |
| BIMCO | Baltic and International Maritime Council Organization |
| CIP | Critical Infrastructure Protection |
| CM | Communications Management |
| CSF | Cybersecurity Framework |
| CUI | Controlled Unclassified Information |
| DoD | U.S. Department of Defense |
| ESCSWG | Energy Sector Control Systems Working Group |
| FERC | Federal Energy Regulatory Commission |
| ICS | industrial control systems |
| IMO | International Maritime Organization |
| IP | Incident Preparedness |
| IRT | Incident Response Team |
| IT | information technology |
| MRE | marine renewable energy |
| NA | Network Architecture |
| NERC | North American Electric Reliability Corporation |
| NIST | National Institute of Standards and Technology |
| OT | operational technology |
| PE | Physical and Environment |
| PNNL | Pacific Northwest National Laboratory |
| RM | Risk Management |
| RMF | Risk Management Framework |
| SD | Security Development |
| SP | Special Publication |

# Contents

# Figures

# Tables

# 1.0 Introduction

Cyber vulnerabilities affecting the energy sector are inherent because of the reliance on industrial control systems and information technology (IT) to optimize operations and maintenance activities. The cyberattacks can vary from the insertion of malware in networks via phishing emails, introduction of a virus in vendor-controlled devices, or initiation of a distributed denial of service attack that could cripple an organization's network [2].

The threat of cybersecurity attacks within maritime transportation, the energy grid, and renewable energy industry is also attracting more attention [3,4]. Marine renewable energy (MRE) systems are a new and emerging form of energy that use IT and operational technology (OT) devices that are just as susceptible to cyberattacks as other sectors that leverage these capabilities. Implementing cyber and physical security of MRE systems is challenged further because of the geographical location of these systems that rely on ocean tides (tidal energy), waves (wave energy), currents (ocean current energy), salinity gradients, and temperature gradients (ocean thermal energy conversion) to generate the energy needs.

This report describes cybersecurity best practices that should be implemented to protect IT/OT systems in MRE systems. The cybersecurity measures are based on determining the cybersecurity risk using the methodology in the Pacific Northwest National Laboratory (PNNL) Report PNNL-29802, *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems* [1]. The cybersecurity best practices are developed using insights from industry guidance on protecting industrial control systems (ICSs) in both the energy and maritime industry.

Section 2.0 of this report provides the background of types of ICS (IT/OT systems) used in MRE systems, the different cybersecurity governances that apply to MRE systems and their end use, and the graded approach to determining a risk categorization for an MRE system described in PNNL Report PNNL-29802.

Section 3.0 describes the approach used to develop the cybersecurity best practices to implement on MRE systems. This section discusses the different techniques to protect IT/OT systems and use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and insights from other cybersecurity guidance developed for the energy industry [8].

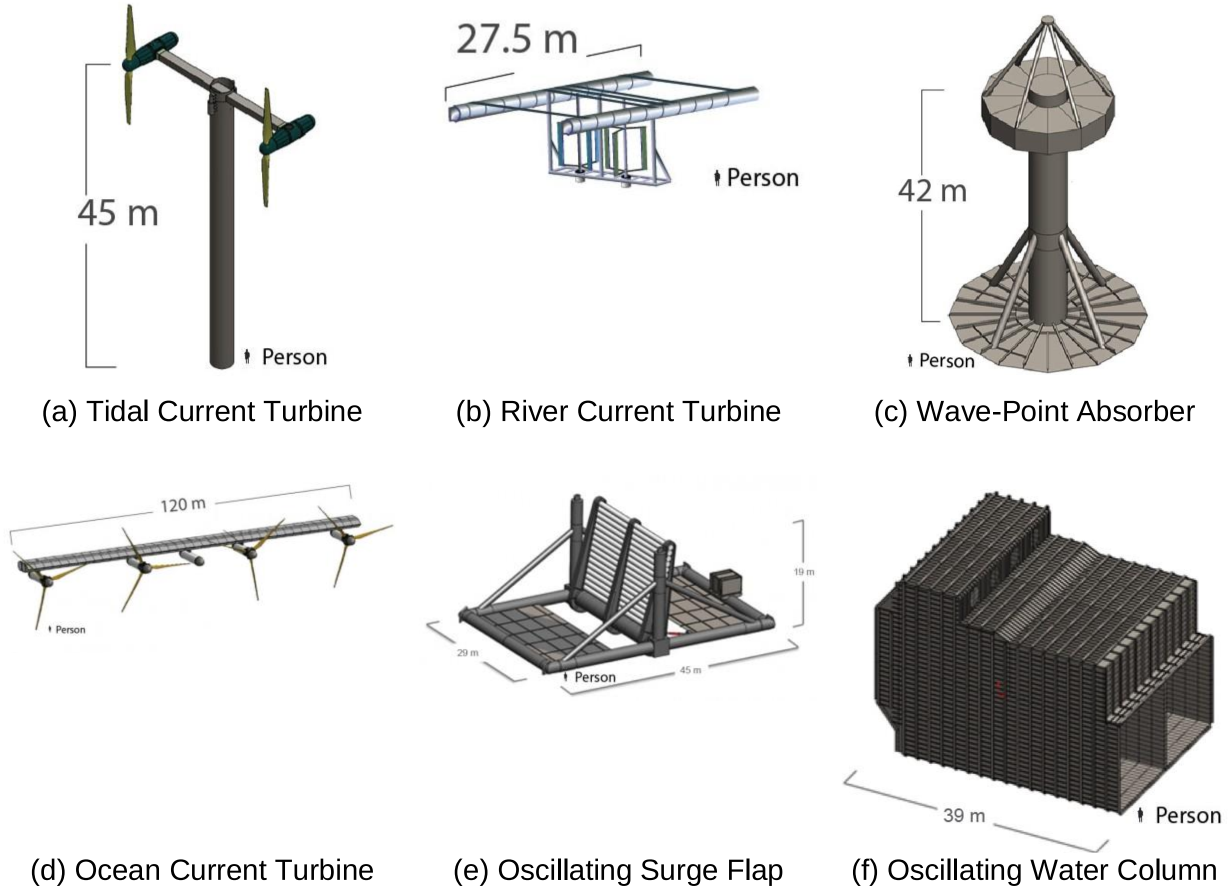
Section 04.0 describes the resultant cybersecurity best practices that MRE system developers and end users can implement to protect their assets based on the risk categorization.

# 2.0 Background

This section describes the types of information and operation technology used in MRE systems, the different authorities that may govern the MRE system's operation, and the elements that contribute to the cybersecurity risk of an MRE system.

## 2.1 Information and Operational Technology in MRE Systems

The MRE systems under the purview of this guidance include wave, tidal, ocean current, and riverine energy devices. Figure 1 includes illustrations of six reference models of MRE device design types that have been developed as open-source reference model designs to provide a methodology for design and analysis of MRE technologies (including benchmarking performance and modeling for estimating capital costs, operational costs, and leveled costs of energy) [5]. While these reference models are examples of potential MRE device designs, they do not represent the full breadth of full MRE designs currently being developed.



(a) Tidal Current Turbine (b) River Current Turbine (c) Wave-Point Absorber

(d) Ocean Current Turbine (e) Oscillating Surge Flap (f) Oscillating Water Column

Figure 1. Illustrations of MRE Reference Models [5]

Based on the information received from the Portal and Repository for Information on Marine Renewable Energy,[1] MRE developers, and MRE test sites, a select number of assets (e.g., hardware, software, computer networks, communication methods, applications, and other OT/IT assets) will be used to support operations and manage MRE stakeholder data (i.e., collected, used, developed, received, transmitted, and stored). Typical MRE system assets are listed in Table 1 and need to be protected from cyber-threat actors.

Table 1. Typical Assets on an MRE System

| Types of Assets | Typical Examples |
|---|---|
| Hardware Endpoints | Operator/Engineer Workstations<br>Servers<br>Safety Instrument System/Protection Relay |
| Human-Machine Interface Application | Mobile Devices<br>Physical Access |
| Network/Communication Equipment | Routers<br>Switches<br>Terminal Servers<br>Gateways<br>Cellular/Satellite<br>Wireless/Bluetooth |
| Field Controllers | Programmable Logic Controllers<br>Field Devices<br>Sensors<br>Actuators<br>Intelligent Electric Devices<br>Remote Terminal Units |
| Other | Security Appliances<br>Test Equipment<br>Peripheral Devices<br>Handheld Configuration Devices |

MRE developers reported that their devices could be continuously or intermittently monitored and controlled from a remote location. MRE systems could also have onboard personal computers for offloading control functions from the programmable logic controllers. Some MRE developers indicated the types of security that are currently implemented (i.e., log-in password protection, management of accounts and sessions, encryption of communications, authentications, malware protection, firewalls, intrusion detection, and physical security). One MRE developer also reported that a cloud computing service will be used to store data.

There are two thematic areas of potential applications for MRE systems within the blue economy shown in Table 2 below: 1) powering marine applications and devices at sea and 2) powering resilient coastal communities. MRE systems are used as a cost-effective alternative to power marine applications and markets operating in deep water (e.g. greater than 100 meter depth) that may extend beyond the Outer Continental Shelf (OCS) where the delivery of power can be both expensive and challenging. For example, an offshore marine hydrokinetic project on the Outer Continental Shelf would likely use wave- or ocean-current-based technologies [23] such as a wave-point absorber or ocean current turbine to power marine applications and devices at sea. Potential markets include ocean observation and navigation, underwater vehicle recharging, offshore marine aquaculture, marine algae, and seawater mining. MRE systems are

[1] https://openei.org/wiki/PRIMRE

also used to provide electricity to coastal communities and facilities. Near-shore marine hydrokinetic projects are likely to implement an MRE technology design such as a tidal current turbine, oscillating surge flap, or oscillating water column. Potential markets include desalination, coastal resiliency and disaster recovery, and isolated power systems (community microgrids). Additional details on the four near-term markets and additional markets not explicitly discussed herein are provided in the U.S. Department of Energy report titled *Powering the Blue Economy; Exploring Opportunities for Marine Renewable Energy in Maritime Markets* [6].

Table 2. Near-Term Blue Economy Markets [6]

| MRE Systems | Function | Markets |
|---|---|---|
| Ocean Observation and Navigation | *Provide power to ocean observation and navigation systems whose use is often limited by battery capacity, data storage, and transmission to shore* | • National Oceanic and Atmospheric Administration<br>• U.S. Department of Defense (DoD) – Navy, Army Corps of Engineers, Coast Guard<br>• Coastal ports (government entities or public-private partnerships) |
| Underwater Vehicle Recharging | *Provide power for underwater charging and docking stations of underwater vehicles whose mission ranges and durations are often limited by battery-power capacity* | • National Oceanic and Atmospheric Administration<br>• DoD – Navy, Defense Advanced Research Projects Agency<br>• U.S. Department of Homeland Security |
| Power to Coastal Communities | *Provide power to coastal desalination facilities that provide drinking water to communities* | • Municipalities already deploying or building desalination facilities to mitigate drought or water security risks |
| | *Provide power for remote, isolated communities (including coastal communities, military bases, and resorts) that often depend on expensive diesel fuel for lighting, water pumping, and wastewater treatment* | • Remote/islanded or isolated communities or resorts that have microgrid power systems<br>• DoD – Defense Advanced Research Projects Agency, Environmental Security Technology Certification Program, Strategic Environmental Research and Development Program<br>• Energy Resilience and Conservation Investment Program |

As of the writing of this report, no clear cybersecurity standards or tailored best practice guidance was identified for the MRE industry that address safeguarding MRE systems through the life cycle (design, construction, operation, and decommissioning). However, this guidance builds on cybersecurity frameworks and energy industry standards to provide a consistent approach for MRE owners and operators to implement as a foundation for the MRE system development life cycle. The control systems installed in MRE system designs are susceptible to cyberattacks, which could result in disrupting the ICS operation (i.e., blocking or delaying flow of information through the ICS networks), changing control logic or information to the commands, modifying the software or configuration settings, and interfering with the operations of the control systems or equipment protection systems [16]. This report identifies cybersecurity best practices that will mitigate potential cyber threats to the MRE systems.

## 2.2 Cybersecurity Governance for Different MRE Users

In the United States, the Federal Energy Regulatory Commission (FERC) under the authority of the Federal Power Act [20] has jurisdiction to issue licenses over marine and hydrokinetic[2] projects on navigable waters (approximately within three nautical miles of shore) and over any projects with an onshore grid connection.[3] The Bureau of Ocean Energy Management administers leases over federal marine projects on the Outer Continental Shelf between the seaward extend of state and federal jurisdictions. [30] The Marine and Hydrokinetic Renewable Energy Act further stipulates that pursuant to Part I of the Federal Power Act, FERC authorizes and regulates nonfederal hydropower projects [24]. The term *marine hydrokinetic* applies to technologies under the Bureau of Ocean Energy Management's leasing responsibility and FERC's licensing responsibility, primarily referring to ocean wave and ocean current technologies [23]. As such, cybersecurity for MRE systems and their end use will be governed by the authoritative agency. The different authoritative agencies are described in the literature review for marine energy regulatory process documented in report PNNL-28608, *Marine Hydrokinetics Regulatory Processes Literature Review* [29]. The cybersecurity best practices developed in this report would be supplemented by the cybersecurity governing authority, as appropriate.

**Marine Hydrokinetic Renewable Energy:**

A form of hydropower that generates energy from free-flowing waters, such as waves, currents, an estuary, or a tidal area and from the free-flowing water in a river, lake, or stream. marine hydrokinetic differs from conventional hydropower in that it generates energy without the use of a dam or other impoundment. [24]

Because cybersecurity requirements are mandated by the appropriate organizational governance, the end user should follow the federal or nonfederal guidance that the MRE stakeholder represents. By extension, MRE devices under the cyber protection requirements of certain MRE stakeholders must follow the governance model for the end user. This report reviewed cybersecurity governance models (discussed in Sections 3.2 to 3.5) related to federal

[2] Marine energy and hydrokinetic energy are often used interchangeably with MRE.

[3] https://tethys.pnnl.gov/regulatory-frameworks-marine-renewable-energy

## State Jurisdiction

Texas and the Gulf coast of Florida are extended 3 marine leagues (9 nautical miles) seaward from the baseline from which the breadth of the territorial sea is measured. Louisiana is extended 3 U.S. nautical miles (U.S. nautical mile = 6080.2 feet) seaward of the baseline from which the breadth of the territorial sea is measured. All other States' seaward limits are extended 3 International Nautical Miles (International Nautical Miles = 6076.10333 feet) seaward of the baseline from which the breadth of the territorial sea is measured.

## Federal Jurisdiction

The seaward limit is defined as the farthest of 200 nautical miles seaward of the baseline from which the breadth of the territorial sea is measured or, if the continental shelf can be shown to exceed 200 nautical miles, a distance not greater than a line 100 nautical miles from the 2,500-meter isobath or a line 350 nautical miles from the baseline.

and nonfederal stakeholders, various end users, and the MRE devices they support to develop baseline security controls that can be adopted by any MRE organization.

Figure 2 below shows federal agency stakeholders and their end-user components alongside a notional set of non-federal stakeholders and their potential subordinate end-user types. In this example, the Department of Energy functions as the federal agency stakeholder providing organizational oversight and governance for the Water Power Technologies Office. Conversely, an organization, such as North American Electric Reliability Corporation (NERC), developing cybersecurity requirements for the protection of the bulk power system functions as a nonfederal stakeholder that may oversee cybersecurity requirements for a private or public utility. In both federal and nonfederal examples, each stakeholder must follow the appropriate cybersecurity governance model dictated by the federal agency or governing organization body.

In some cases, nonfederal stakeholders do not have such oversight and are therefore regulated by the requirements set forth at an organization’s enterprise level. Therefore, it is important that MRE organizations follow a set of cybersecurity requirements based on a framework that (1) aligns to existing federal governance requirements (e.g., NIST Cybersecurity Framework [CSF]) [8] and nonfederal regulations and (2) provides IT/OT cybersecurity measures and controls that may be voluntarily adopted by owners and operators of MRE critical infrastructure to help them identify, assess, and manage cyber risks.

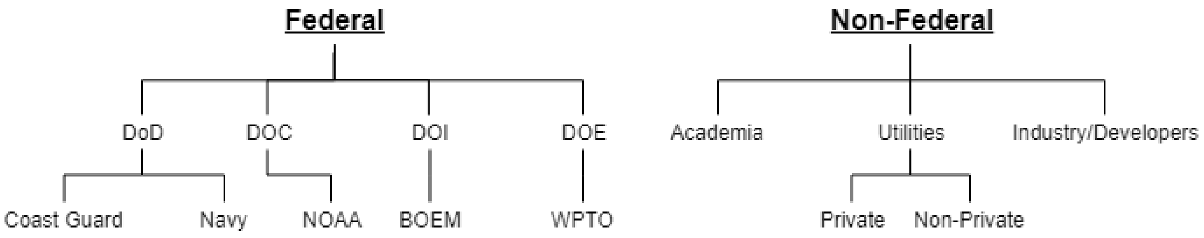


Figure 2. Example Federal and Nonfederal Stakeholders and MRE End Users

The MRE cybersecurity best practices adhere to the NIST CSF and provide different MRE end users an adaptable approach to support cyber governance for federal and nonfederal stakeholders. Additionally, the MRE cybersecurity best practices will benefit MRE end users by providing built-in flexibility for the implementation of cybersecurity controls, a risk-based cybersecurity guidance, and a set of informative references that conform to industry best practices and standards. Investing in best practices in the design iteration, before systems are deployed in the field, will be significantly more cost effective for the developers. The MRE cybersecurity best practices described in this report use insights from governance documents and are enhanced by incorporating other best practices implemented in other similar renewable energy systems (e.g., photovoltaic-array solar, wind, etc.). Finally, the cybersecurity guidance in this report has been tailored for protection of MRE systems, their operating environment, and their intended end use.

## 2.3 MRE System Cybersecurity Risk Levels

PNNL Report PNNL-29802, *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems* [1] evaluates the different cyber threats and vulnerabilities that MRE systems could experience based on the types of assets and operational configuration. Figure 3 illustrates different example attack pathways a cyber-threat actor can use to affect an MRE system's network. The vulnerability to a cyberattack is based on digital assets, geography of the MRE system, physical accessibility, connectivity, and the existence of dedicated personnel to manage cybersecurity of the MRE system and the networks.

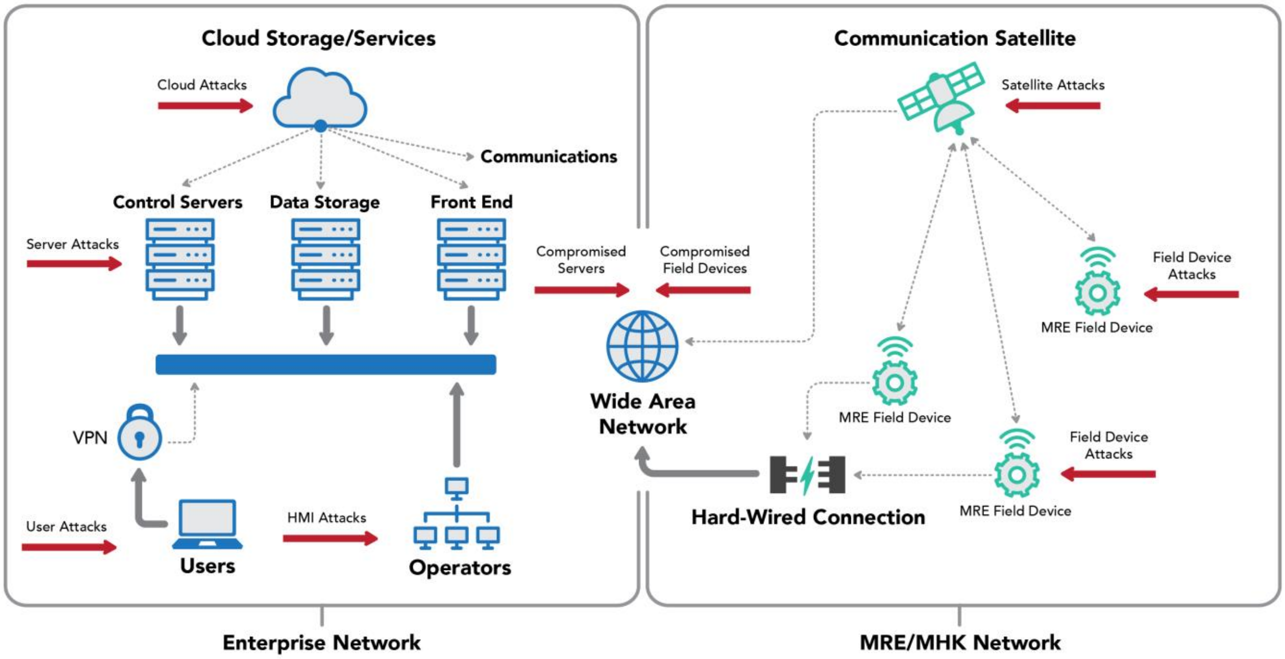


Figure 3. Example Attack Pathways into a Network Architecture

The cybersecurity risk of the MRE system will dictate the security measures necessary to protect the MRE system assets and the owner/operator. Section 3.6 discusses the different elements that influence the vulnerability of a system (e.g., assets, geography, physical protection, connectivity, maturity of security controls, access management, and cybersecurity culture) and the consequences of a cyberattack (e.g., impact to mission, MRE system, data loss, consequential impacts, financial liabilities). The cybersecurity best practices developed in this report are identified for three different risk levels. Therefore, it is important for MRE system owners to understand the threats to their systems, the vulnerability of their systems, and the consequences to the business and mission.

# 3.0 Approach

One of the Department of Energy's highest priorities is to protect America's energy systems from cyberattacks and other risks by using risk-based methods to prioritize activities to support risk management responsibilities for the energy owners and operators [7]. As such, ensuring the cybersecurity of energy systems is a shared responsibility between the private sector and all levels of government, whereby owners and operators of MRE systems within the energy infrastructure have the primary responsibility for managing cybersecurity risks [4,7]. For example, owner/operator(s) may have contractual obligations to ensure the confidentiality, integrity, and availability of energy generation by the MRE systems and assets in order to protect mission/business functions, meet energy resiliency requirements, and provide for the safe reliability of power to downstream end users (e.g., utilities, service agreements, customers). In other cases, the MRE system owner/operator(s) may function as the information system owner responsible for the categorization, selection, implementation, and continuous monitoring of security controls MRE systems and assets, in accordance with the demands of upstream stakeholders (e.g., government and industry partnerships, stakeholders and public/private co-ops). Report PNNL-29802 identified an approach that MRE system owners and operators can use to determine cybersecurity risk based on the vulnerability of the MRE system to protect from known threats and the impact that a cyberattack would have on the end user's mission and business objectives [1].

The first step to developing the cybersecurity guidance document is to know the types of threats that MRE systems would need to protect against. Common threat vectors identified for MRE systems include malicious activities (i.e., denial of services, malware, ransomware, etc.), sniffing communication traffic, vulnerability scanning, physical attacks (i.e., sabotage, theft, unauthorized access, etc.), infrastructure or component failures/malfunctions, improper network architectures, disruption of service providers, and disaster-related threats (e.g., shipwrecks or tsunamis) [1]. Common techniques to protect the MRE system from known cyber threats were obtained from sources that focus on cyber threats, such as Dragos and MITRE [10,11,12].

The second step involves specifying cybersecurity program requirements and security controls to mitigate known cyber threats to MRE systems. The core functions of NIST CSF (Figure 4) are used to develop the security measures necessary to **identify** assets, **protect** critical systems, **detect** incidents, **respond** to incidents, and **recover** to normal operations [8].

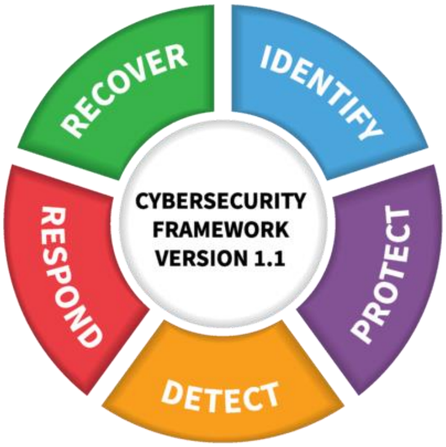


Figure 4. NIST Cybersecurity Framework Core Functions [8]

The premise of CSF is to provide organizations a standard that includes business drivers and cybersecurity best practices for critical infrastructure owners and operators to establish a replicable risk-based and cost-effective approach to protect their systems and information from cybersecurity risk. This approach includes consideration of cybersecurity risks in IT/OT systems, cyber-physical systems, and connected devices using emerging technology, including industrial internet of things. The use of these technologies relies on interconnectivity and communication methods that pave the way for potential security vulnerabilities to be leveraged by threat actors and hacktivists alike. This ultimately increases the risk to operations affected by a cyberattack.

Prior to CSF, NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations* was developed in 2010 to provide guidance to federal agencies and contractors on implementing a cybersecurity risk management program [9]. The NIST Risk Management Framework (RMF) describes a process for managing cybersecurity risk and is intended primarily for the government. The security controls in RMF can be used with CSF. The two different frameworks complement each other.

In addition to NIST CSF and RMF, other cybersecurity guidance documents were reviewed to develop the cybersecurity best practices for MRE systems (Figure 5). NIST SP 800-60 Volume II, *Guide for Mapping Types of Information and Information Systems to Security Categories:* Appendices, Volumes I and II, provide guidelines on mapping certain types of information systems to security categories and the rationale. Table D-2 of NIST SP 800-60, Volume II [27] recommends that the security categorization of information related to energy supply be categorized as “Low,” “Moderate,” and “Moderate,” respectively, for confidentiality, integrity, and availability. In some cases, MRE systems that support mission-critical procedures may be categorized as “High” for integrity and availability. Section D.7 in Appendix D of NIST SP 800-60, Volume II provides information on the basis for selection of the different categories for confidentiality, integrity, and availability.

Guidance for the energy sector, such as the *Cybersecurity Procurement Language for Energy Delivery Systems* [13], was developed by the Energy Sector Control Systems Working Group (ESCSWG) to address specific procurement language to include in contracts with energy deliver system providers. The Critical Infrastructure Protection (CIP) standards developed by NERC are provided to electric utility owners to protect their energy-generating facilities from affecting the bulk electric system (BES) if a cyberattack occurs. Other cybersecurity guidance documents developed by organizations dedicated to protecting the marine industry, such as the International Maritime Organization (IMO), Baltic and International Maritime Council Organization (BIMCO), and American Bureau of Shipping (ABS) provide additional security controls that are unique to the marine industry. The following subsections provide background on the documents that were used to develop the MRE system cybersecurity best practices.

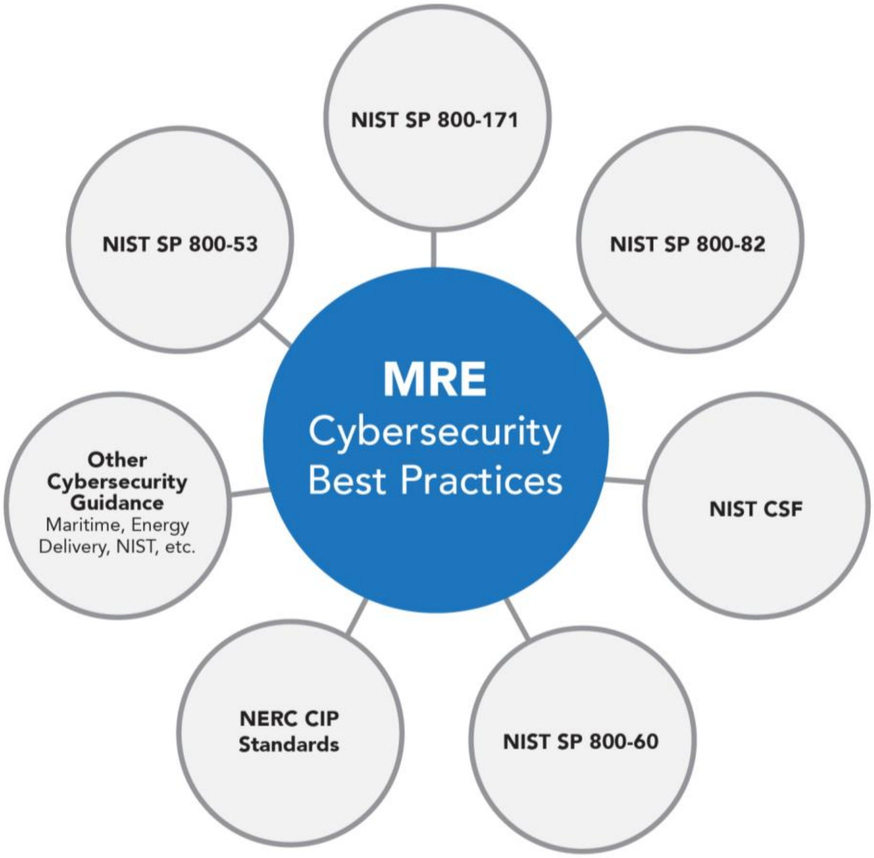


Figure 5. Industry Guidance to Inform MRE Cybersecurity Best Practices

## 3.1 Mitigation Strategies for Cyber-Threat Tactics and Techniques

Dragos and MITRE are organizations known to keep abreast of cyberattacks on ICS and IT/OT environments. In a report of the 2019 ICS threat landscape [10], Dragos reported an increase in activity targeting ICS and “the associated cyber risks continue to grow and remain at a high level.” Just recently in March 2020, Dragos posted a blog describing how energy organizations continue to be targeted by adversaries that infiltrate networks through successful insertion of ransomware or via trusted connections between vendors and contractors [14]. A risk-based and ICS-specific cybersecurity program will include ICS-specific monitoring, threat detection, and response. ICS environments include assets and configurations that are designed to process data and equipment operations using protocols and other distinctive characteristics where traditional IT enterprise monitoring systems perform ineffectively [14]. Dragos encourages asset owners and operators to monitor malicious behavior within the ICS, such as callouts to the internet or internet-routable Internet Protocol addresses, new account creation, new devices on the network, and unauthorized configuration changes [14]. In 2017, MITRE started work on a new initiative that evaluated unique threat behaviors targeting ICS networks because ICS technology works differently than enterprise technology.

MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) matrices for ICS [11] and enterprises [21] provide a framework for security managers to assess and improve their security controls for ICS and OT environments. MITRE provides a knowledge base of adversary tactics, techniques, and mitigation methods that is used to develop security controls to prevent cyber threats to MRE systems. For example, adversaries may send phishing messages or emails to elicit sensitive information or gain access to the MRE systems, or they may insert malware through malicious attachments or links to gather credentials. Mitigation strategies include installing antivirus/anti-malware or network intrusion prevention software, blocking access to websites or attachments that can be used for phishing, or training the organization's staff to identify social engineering techniques and phishing emails. Mitigation strategies for threats identified for MRE systems are evaluated to verify that they are included in the cybersecurity best practices.

## 3.2 Applicable NIST Guidance Documents

NIST is a known resource for technological advancement and security for many organizations (federal and nonfederal). NIST also produces standards and guidelines that federal agencies can use to meet the requirements of the Federal Information Security Management Act. The recommended security controls in NIST SPs that are relevant to the ICS, energy, marine, and critical infrastructure sectors were evaluated for applicability to protect MRE systems from known adversarial threats.

Specific guidance documents from NIST were chosen as source documents for the cybersecurity best practices for MRE systems. The NIST documents discussed in the following subsections were chosen as input to the development of the MRE cybersecurity documents. A summary of the NIST documents and the basis for selecting them as input to securing MRE systems follows.

### 3.2.1 NIST Cybersecurity Framework

The NIST CSF was initially prepared and issued in 2014 in response to Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*.[4] This order directed NIST to collaborate with industry leaders to develop a framework to protect critical infrastructure, such as utilities providing energy and water and sectors covering transportation, financial services, communications, healthcare and public health, food and agriculture, chemical and other facilities, dams, key manufacturers, emergency services, and several others. CSF is a voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders. Version 1.1 was released in 2018 and includes an update to many of the best practices and standards established in the first release.

Presidential Policy Directive 21 [19] defines **critical infrastructure** as:

"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Because of the comprehensive nature of the CSF, the timely and recent applicability of its publication, and the detail in which each control is mapped to other source documents and mitigation strategies, CSF was chosen as one of the pillar sources to construct MRE Systems

[4] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity,* was issued on February 13, 2013 to enhance the security and resilience of the US critical infrastructure. Retrieved at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

Framework with. Specifically, MRE systems that generate power fall under the category of critical infrastructure as defined in CSF, which means it was especially created with MRE systems in mind. In addition, CSF contains applicable guidance for federal agencies. As such, the cybersecurity programs for MRE systems that are used by federal agencies would have to follow the CSF.

### 3.2.2 NIST SP 800-53

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* [15], is a key source of guidance for choosing effective cybersecurity controls to protect information systems to maintain integrity, confidentiality, and security of federal information systems. It provides a catalog of security controls that organizations, in any sector, any technology, and any operating environment can select to protect information systems and organizations from "a diverse set of threats including hostile cyberattacks, natural disasters, structural failures, and human errors" [15]. NIST SP 800-53 also provides direction on how to "develop specialized sets of controls, or overlays, tailored for specific types of mission or business functions, technologies, or environments of operation" [15]. While NIST SP 800-53 was prepared to protect information systems, it is a commonly cited source of security controls in many regulations, guidance documents, and contracts.

Besides CSF, Special Publication 800-53 was the most prevalent document used as a reference to develop the cybersecurity best practices for MRE systems. The guidance directly informed most of the techniques and security strategies described by Dragos or MITRE to mitigate cyber threats targeting ICS and MRE systems.

### 3.2.3 NIST SP 800-82

In 2011, NIST published SP 800-82*, Guide to Industrial Control Systems (ICS) Security*, which provides guidance on securing ICS, including supervisory control and data acquisition systems, distributed control systems, and other control system configurations to address performance, reliability, and safety requirements [16]. NIST SP 800-82 presents a security control overlay of the catalog of security controls identified in NIST SP 800-53 Revision 4 and is customized to specifically address the characteristics and security needs of ICS/OT systems.

As MRE systems are expected to contain typical energy sector ICS/OT topologies and devices, this document refers to specific security controls to mitigate risks recognized within the ICS/OT field of systems.

### 3.2.4 NIST SP 800-161

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organization* [17], was created to protect against the risks to information and communications technology products and services used within MRE systems. These risks include systems and software that contain malicious functionality, are counterfeit, or are otherwise vulnerable due to poor manufacturing and development practice when used within the supply chain. Cybersecurity risks are introduced to the MRE system owner and operator when there is decreased visibility and understanding of and control over how the technology is developed, integrated, and deployed. Cybersecurity risks are also introduced when there is a lack of transparency in the processes, procedures, and practices that are used to assure the integrity, security, and resiliency of the products and services. NIST SP 800-161 provides guidance on identifying, assessing, and mitigating IT supply chain risks at every level of a given organization.

Much of the MRE design process involves acquiring and implementing technology that is not developed exclusively under the MRE developer, meaning that supply chain risks are some of the more pertinent issues that will need to be addressed by MRE developers. The team used this document when researching to gather supply chain security controls and mitigation strategies.

### 3.2.5 NIST SP 800-171

MRE systems that are used by federal agencies may house controlled unclassified information (CUI) that can have a direct impact and importance to federal agencies. This information, and the protection of that information while it is being housed within a non-federal agency, can affect the federal agencies' ability to conduct essential missions and operations and is required by the regulations[5] to protect. As such, NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* [18], was created to address specific safeguarding requirements for protecting the confidentiality of CUI listed in the CUI registry. These requirements apply to all components of nonfederal systems and organizations that process, store, and/or transmit CUI or that provide protection for such components. These security requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies in nonfederal organizations.

The team specifies the need to follow NIST SP 800-171 for MRE systems that house CUI and supply power to a federal agency. As energy-related information can fall within the CUI category, information collected or transmitted through the MRE system must, in the case of federal contractors, adhere to the protections and mitigations set forth in this document. MRE systems that do not support federal agencies only need to follow the cybersecurity governance required by the end user involving the protection of sensitive information (e.g., official use only, proprietary).

## 3.3 NERC CIP Reliability Standards

The NERC CIP Cybersecurity Reliability Standards[6] are designed to protect the reliability of the U.S. BES against cybersecurity risks. The NERC CIP standards apply to an MRE system owner/operator if it is responsible for transmission of power from the MRE system to BES (i.e., MRE system provides power coastal communities via the electrical grid governed by FERC). The NERC CIP Reliability Standards implement a tiered approach to categorize assets as high, medium, or low risk to bulk power system reliability if compromised. High-impact systems have large control centers; medium-impact systems include smaller control centers, ultra-high voltage transmission, and large substation and generating facilities. A simultaneous cyberattack on multiple electric grid facilities can have the effect of instantaneously dropping large amounts of load or generation from the grid [22]

It is important to understand that FERC's mission is to safeguard the operation of the wide-scale interconnected power grid (i.e., the BES) and *not* the operation of smaller MRE assets or the distribution of electrical power to customers (e.g., stakeholder installations, industrial areas, or residential neighborhoods). The NERC CIP Reliability Standards only apply to generation that is considered part of the BES. For generation, the threshold for the most stringent requirements is 1500 MW, while less stringent requirements apply to individual generators greater than 20 MW,

[5] Federal Acquisition Regulation (FAR) 52.204-21 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 (https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm).
[6] NERC CIP Standards can be retrieved at https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

or generation plants[7] greater than 75 MW,[8] with some exceptions. In the case of energy generation less than 75 MW that is located “behind the retail meter” (on the customer’s side) of stakeholder installations (i.e., supplying power to the installation but not outside the installation), BES Exclusion E2[9] may be applied to exclude the generation from being considered BES and therefore from being required to comply with the NERC CIPs. Regional utilities are mandated to enforce the reliability standards as part of NERC’s Compliance Monitoring and Enforcement Program, which was developed under Section 215(c) of the Federal Power Act.[10]

## 3.4 Energy Sector Cybersecurity

In 2014, ESCSWG, which comprises a multidisciplinary team representing the government (Department of Energy, U.S. Department of Homeland Security, FERC), PNNL, and industry (Duke Energy, Edison Electric Institute, the Electric Power Research Institute, Energetics Incorporated, Independent Electric System Operator [Ontario, Canada]) developed cybersecurity procurement language that was designed to lay the groundwork for establishing a baseline criteria for an energy-based organization [13]. The document included cybersecurity requirements to protect individual components of energy delivery systems (e.g., programmable logic controllers, digital relays, and remote terminal units), energy delivery systems (e.g., a supervisory control and data acquisition system, energy management system, or distributed control systems), and assembled or networked energy delivery systems (e.g., an electrical substation [transmission and distribution] or a natural gas pumping station). The ESCSWG document was based on industry good practices; NIST SP 800-82 Rev. 2, *Guide to Industrial Control Systems (ICS) Security* [16]; NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* [9]; and a number of other cybersecurity standards and guidance documents.

The recommended set of cybersecurity requirements developed by ESCSWG were reviewed and referenced in the MRE cybersecurity best practices, as appropriate.

## 3.5 Maritime Cybersecurity Guidance Documents

As MRE devices operate in near-identical conditions and locations as marine ships and offshore operations and share many of the same threats and attack vectors, cybersecurity guidance from IMO was considered by the team, specifically the preferred guidance notes from BIMCO concerning cybersecurity onboard ships and the ABS guidance notes on the Application on Cybersecurity Principles to Marine and Offshore Operations. These documents were studied by the team as the discovered applicable threats were prioritized and as a means of identifying mitigation strategies.

### 3.5.1 IMO Guidelines on Maritime Cyber-Risk Management

IMO[11] is a United Nations agency that manages the safety and security of international shipping and legal matters involving maritime traffic. With 174 member states, it is the largest marine

[7] While there is no formal definition of a “plant,” plants are generally understood to contain multiple individual generating units, such as natural gas generators, wind turbines, or solar panels at a single location.

[8] See NERC Glossary, Bulk Electricity Definition, Inclusion I2.

[9] See NERC Glossary, Bulk Electricity Definition, Exclusion E2.

[10] Section 215(c) of the Federal Power Act can be retrieved at https://www.ferc.gov/sites/default/files/2020-05/E-18_20.pdf.

[11] http://www.imo.org/en/About/Pages/FAQs.aspx.

shipping-related organization. In 2017, IMO adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems, which states that all approved safety management systems should take cyber-risk management into account and that administrators should make sure that cyber risks are addressed no later than January of 2021. Later in the year, IMO then developed guidelines with recommendations on cyber-risk management for current and emerging cyber threats and vulnerabilities. [25] These guidelines were consulted by the research team to make sure no gaps existed between marine-specific cyber risk management and energy sector specific cyber-risk management.

### 3.5.2 Baltic and International Maritime Council Organization Cybersecurity Onboard Ships

BIMCO[12] is the world's largest direct-membership organization for shipowners, charterers, shipbrokers, and agents, with around 60% of the world's total merchant fleet having membership. BIMCO is based in Denmark, with other offices in Athens, Singapore, and Shanghai. In response to the IMO cybersecurity guidelines, BIMCO, in partnership with other shipping organizations, created *The Guidelines on Cyber Security Onboard Ships* [25], intended to assist companies in formulating their own approaches to cyber-risk management onboard ships. Throughout the document, specific use cases and examples of cyber risks unique to the marine industry are presented; the MRE team consulted with the marine industry when creating and categorizing possible risks to MRE systems. In addition, elements of BIMCO's cyber-risk management approach were examined by the PNNL team to develop the cybersecurity best practices.

### 3.5.3 ABS Cybersecurity Principles to Marine and Offshore Operations

ABS[13] is a classification society whose stated mission is to promote the security of life, property, and the natural environment through the development of standards for the design, construction, and operational maintenance of marine and offshore assets. ABS created the *Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations* [26] to provide best practices and recommendations to both marine and offshore organizations and enable them to take verifiable steps to protect an asset included in their cyber-connected systems from cyber intrusions. Its specific application is for implementation on ships, platforms, vessels of any type, and support facilities.

Considering the targeted nature of the security guidance to offshore platforms, the team analyzed this source document for any cyber controls that would apply to the MRE industry and that had not been covered in other source materials.

## 3.6 Determining Requirements for Each Risk Level

The MRE system risk model determines the risk levels based on likelihood of vulnerability and the consequence to an MRE system (refer to Section 2.3 for the description of the metrics that contribute to vulnerability and the factors that are measures in consequence). As shown in Table 3, the risk is identified in three progressive levels depending on the vulnerability (Low, Moderate, or High) and the consequence (Low, Moderate, or High). The progressive risk levels provide MRE system end users the flexibility to ascertain the security controls necessary to prevent and mitigate a potential cyberattack. The MRE system owner/operator prioritizes risk based on a valuation of implementing security controls based on impact.

[12] https://www.bimco.org/about-us-and-our-members

[13] https://ww2.eagle.org/en/about-us/safety.html

Table 3. MRE System Cybersecurity Risk Ranking Chart

| Vulnerability | Consequences of Cyberattack | | |
|---|---|---|---|
| | LOW | MODERATE | HIGH |
| LOW | 1 | 2 | 3 |
| MODERATE | 1 | 2 | 3 |
| HIGH | 2 | 3 | 3 |

Determining the risk level of an MRE system, its configuration, and end use is paramount to the security needed to protect the assets. Section 4.1 discusses the elements of each risk level further.

# 4.0 Results

The NIST RMF described in NIST SP 800-37 [9] describes a process for managing cybersecurity risk for IT/OT systems and organizations. The NIST RMF process is a cyclical process that is followed throughout the life cycle for a system or organization. A similar risk management framework process is developed for managing the cybersecurity of the life cycle of the MRE system and the owner (end users) and is shown in Figure 6.

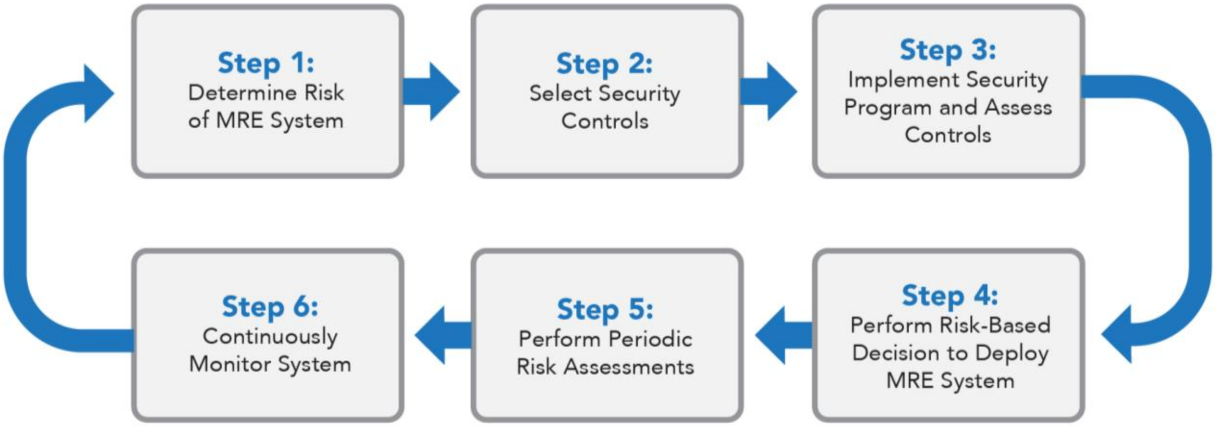

Step 1:
Determine Risk of MRE System
Step 2:
Select Security Controls
Step 3:
Implement Security Program and Assess Controls
Step 4:
Perform Risk-Based Decision to Deploy MRE System
Step 5:
Perform Periodic Risk Assessments
Step 6:
Continuously Monitor System

Figure 6. MRE System Cybersecurity RMF

The six steps of the MRE Systems Cybersecurity RMF provide guidance on implementing a risk-based cybersecurity program.

- Step 1 involves determining the cybersecurity risk of an MRE system (e.g., Risk Level 1, 2, or 3) using the Risk Categorization Worksheet described in Appendix C. Section 4.1 discusses the method to determine cybersecurity risk of an MRE System [1].
- Step 2 involves selecting the security best practices commensurate with the risk as described Section 4.2.
- Step 3 involves implementing the security measures to protect the systems and organization.
- Step 4 involves working with end users' leadership to deploy the MRE system after verifying the security controls are successfully implemented, including development of the policies and procedures to manage aspects of the cybersecurity program.
- Steps 5 and 6 involve post-operation maintenance of the cybersecurity program by respectively performing periodic risk assessments and monitoring the systems on an ongoing basis to verify the effectiveness of the security measures and document any changes to the system and environment of operation and report the security and privacy posture of the system.

When a change in risk is identified during steps 5 and 6, repeat steps 1 through 4 in the MRE Systems Cybersecurity RMF to secure the system and organization, as needed, to minimize cybersecurity risk. MRE system owners and operators develop and manage their cybersecurity program using the RMF (Figure 6) during initial deployment and daily operations throughout its life cycle.

## 4.1 Categorize the Cybersecurity Risk

The initial step of the MRE System Cybersecurity RMF (Step 1), shown in Figure 6, is to categorize the cybersecurity risk of the systems and assets. The risk is based on the vulnerability of a cyberattack and the consequences that an incident would have on the MRE system owner and operator. An approach used to assess the cybersecurity risk was developed by PNNL in report PNNL-29802, *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems* [1]. Different factors contribute to the risk of a cyberattack.

Cybersecurity risk is a measure of a cyberattack (i.e., vulnerability of MRE systems to known threats) and the consequence an attack would have on the end user. Different measures of impact (low, moderate, or high) that a cyberattack could impose on the MRE system and end user [1] are used. The metrics used to qualitatively categorize the vulnerability of an MRE system to cyber-threats as either LOW, MODERATE, or HIGH are as follows:

1. **IT/OT Assets and Network Architecture:** The diverse designs of MRE systems are factored into the vulnerability. MRE systems that do not have any IT/OT assets limit the opportunity for cyber threats to occur and hence would be graded LOW. However, MRE systems that have IT/OT assets and a network architecture begin introducing threat vectors that provide some level of vulnerability. MRE IT/OT assets and networks that can only be accessed locally are graded MODERATE because of the limited vectors to access the network. MRE systems that can be accessed remotely are graded HIGH because additional threat vectors are introduced because of the need to protect communications between the MRE system and remote location(s).
2. **Geographical Accessibility:** Even though cyberattacks are unconstrained by geography and distance [28], the inherent and diverse geographical location of MRE systems could contribute to a cyber vulnerability because it constrains security controls, such as monitoring capabilities. For example, MRE systems located well below the water surface (e.g. underwater charging stations), above the surface of the ocean (e.g. powering buoys used for oceanwater navigation), or near coastal communities. The diverse locations of the MRE systems contribute to an asset's vulnerability because it provides insights into the physical exposure and difficulty of an adversary gaining access to the system based on terrestrial access points, seasonal weather events, windows of accessibility influenced by sea states, and the need for specialized vessels.  The vulnerability of the MRE system is also dependent on how well the MRE system is physically monitored.  MRE systems located in remote areas and continuously monitored by the owner (i.e., cameras, sensors, etc.) are graded LOW. An MRE system that is monitored with no alarm notifications or is physically monitored periodically (at least weekly) is graded MODERATE. Lastly, an MRE system that is not monitored through electronic or physical means (more than once a week) is graded HIGH.
3. **Physical Accessibility:** The physical protection of an MRE system is dependent on how well physical access to the MRE device/system is controlled. MRE systems have a heightened level of physical security (i.e., LOW vulnerability) if their IT/OT assets are protected by a locked enclosure (e.g., barrier, fence, specialized server container, or conduits for cables) and access to those physical barriers are managed. MRE system designs that are protected by a secured enclosure (barrier, tidal fence, or container) but access to these physical barriers is not strictly managed (i.e., group-based access, such as vendors performing maintenance) have a level of vulnerability graded MODERATE because of the increased possibility of not knowing who specifically is accessing the systems. Assets that are not protected by any physical enclosures (barrier, tidal fence, or container) or if the

enclosures are not locked and/or can be accessed by anyone are graded HIGH because the assets would pose a greater risk of unauthorized access.

4. **Connectivity Duration with External Networks:** This metric relates to the duration of connectivity to external networks. MRE systems that do not connect to external networks or connect infrequently (e.g., once a month or less) are deemed to be LOW risk. MRE systems that connect to external networks at least weekly (MODERATE) or continuously (HIGH) have a greater risk of unauthorized access.
5. **Access/User Controls:** Because of the remote environment where MRE systems are located, the method of controlling access and users (accounts) is an important factor to security. Identification and authentication of accounts that are managed (e.g., least privilege established, role-based, multifactor authentication, etc.) provide sufficient protection and reduce the risk  of unauthorized access are graded LOW vulnerability. If identification and authentication of accounts are partially managed (e.g., multiple users on same account allowed, least privilege not established, etc.), then the access/control method is graded MODERATE, and if it is not managed at all, then it is graded HIGH.
6. **Roles and Responsibilities:** An organization’s cybersecurity culture is another metric that is used to evaluate the vulnerability of an MRE system and its operation. An organization that has dedicated staff to manage its cybersecurity program and implementation (e.g., Chief Information Security Officer, incident response roles, etc.) is considered a LOW vulnerability. However, if the organization has a partially dedicated staff to manage cybersecurity (e.g., staff member shares other roles outside of cybersecurity), then it is graded MODERATE because the other responsibilities may affect the effectiveness of managing the cybersecurity program. An organization that does not have dedicated staff or is understaffed to manage its cybersecurity program is graded HIGH.
7. **Security Controls on Hardware and Software:** This measure is intended to qualitatively determine the vulnerability of an MRE system that will be operated by an organization that currently has a cybersecurity program in place. An organization that currently implements preventive (e.g., patch management, encryption, antivirus, or continuous security monitoring, automatic updates, etc.) and detection methods (e.g., host or network intrusion detection, etc.) is considered a LOW vulnerability. If the organization only implements preventive measures (no detection), then it is graded MODERATE. If the organization implements minimal or no controls to protect digital assets and monitor its networks, then it is graded HIGH.

The consequences of a cyberattack need to be evaluated to determine the appropriate cybersecurity risk. Different consequences are assessed to measure the impact that a cyberattack would have on the MRE systems and its end use. The impact varies depending on the assets and networks affected by the cyberattack, the extent of infiltration to the networks and control systems, and the types of information affected. The consequences are assessed qualitatively based on known information at that time. For example, MRE systems that are currently deployed provide power to support federal agency programs, as shown in Table 2. As development of MRE system designs improve and more markets use MRE systems for energy consumption, additional types of consequences may need to be considered. Based on the current market known to date, the consequences are assessed equally and graded LOW, MODERATE, or HIGH with a scale of 1, 2, and 3, respectively, as follows:

1. **Impact on end user’s mission.** This consequence is evaluated in the NIST and DoD RMFs to categorize the security risk of an assets. If the organization can continue to perform its primary functions (i.e., mission is not affected) and a cyber incident has zero to minimal impact on the organization’s function, then the consequence is categorized as LOW. If the cyber incident will significantly affect the effectiveness of the organization’s function, then

the consequence is graded MODERATE. A HIGH impact grade is determined if the cyber incident will affect the organization such that it cannot perform one or more of its primary functions.

2. **Physical Impact to the MRE System.** Because of the remote locations where MRE systems operate, a physical impact consequence was factored into the risk assessment. A cyber incident that would not cause physical damage to ICSs and supporting infrastructure or only minor damage (i.e., redundant controls available, non-digital mechanisms provided such as audio alarms, manual valves to protect the physical boundary) is graded LOW. Consequences that result in significant physical damage to assets, supporting infrastructure, and human safety (e.g., manipulation of controls) is graded as MODERATE impact. Consequences that result in major physical damage to assets and supporting infrastructure and impact to environment (e.g., damage to electric generation and delivery) is graded as HIGH impact.
3. **Loss of data or information (e.g., impact of loss of confidentiality, integrity, and availability).** The consequences of a cyber incident that result in loss of the confidentiality, integrity and availability of data or information that may impact MRE system or end-user operations are also factored into the risk assessment. For example, the impact of sensor data (i.e., malware, compromise of authentication), may affect the integrity or availability of control system response in the MRE systems.   Another example is the impact on a data breach (i.e., social engineering) may result in the loss of confidentiality of business/sensitive information. If the loss of data generated, stored, and transmitted in an MRE system does not affect the mission or end use, then it is graded a LOW impact. Loss of data that will affect the organization's revenue or reputation is graded MODERATE if the impact is minor and HIGH if the impact is significant.
4. **Impact to interconnected networks (e.g., enterprise systems, end user's systems, other ICS networks etc.).** MRE systems that have no connectivity to other networks are graded LOW because impact would be limited to a single network. If different networks are interconnected and connectivity can be isolated (i.e., segmented network), then the impact is graded MODERATE. If connectivity with other networks cannot be isolated, then the impact is graded HIGH.
5. **Financial impact.** Financial impacts (i.e., business costs due to loss of productivity, response to an incident, recovering from an incident, or fines mandated by a regulator) are also factored into the risk assessment. An incident that results in no or low financial impact is graded LOW, significant financial impact is MODERATE, and major financial impact is graded HIGH. The organization defines the criteria for low, significant, or major financial impact based on its business objectives and the financial losses that the organization can accept from a cyberattack.

Appendix C includes the Cybersecurity Risk Categorization Worksheet that MRE system owners and operators can use to determine the cybersecurity risk of the system. As shown in Table 3, the assessment results in a progressive approach to categorizing risk: Risk Level 1 being the lowest risk and Risk Level 3 being the highest risk.

Determining the risk level of an MRE system, its configuration, and end use is paramount to the security needed to protect the assets. A description of each level is provided below:

- **Risk Level 1: Low/Moderate Vulnerability, Low Consequences**

  Physical assets are enclosed in a locked boundary and personnel access is managed and monitored. The IT/OT systems may be simple controls with no connection or minimal connection (once a month) to external networks. Accounts and access to network are managed and authenticated using principles of least privilege and multifactor authentication. These MRE systems may also have staff dedicated to cybersecurity and have a strong culture of continuously maintaining security and safety within the MRE system and the organization. The consequence of a cyberattack on the MRE system may also not adversely affect the end user's business (financial) or mission (operation).

Cybersecurity guidance will involve minimal security controls that cover basic security hygiene (e.g., asset management, business environment, risk management, awareness and training, anomalies and events, and communications).

- **Risk Level 2: High Vulnerability/Low Consequence or Low/Moderate Vulnerability/ Moderate Consequence**

  Physical assets are enclosed in a locked boundary, and personnel access may not be formally managed and monitored. The network for IT/OT systems may involve frequent connection (weekly) to external networks. Accounts and access to network may not be managed, monitored, and authenticated using principles of least privilege or multifactor authentication. The MRE system end user may also have a small number of staff members responsible for cybersecurity or the responsible staff members may have multiple responsibilities within the organization. The consequence of a cyberattack on the MRE system may have a moderate impact on the end user's business (financial) or mission (operation) by affecting the MRE system's function.

  Cybersecurity guidance will involve security measures required for Risk Level 1 and additional risk management controls (vulnerability assessments, risk assessments, supply chain risk management, etc.).

- **Risk Level 3: High Vulnerability/Moderate Consequence or Low/Moderate/High Vulnerability/High Consequence**

  Physical assets are enclosed in a boundary and personnel access may not be formally managed and monitored. The network for IT/OT systems may involve continuous or frequent (daily) connection to external networks or may involve wireless, Bluetooth, radiofrequency, or satellite communications technology. The network may also not have adequate controls (e.g., firewalls or password protection). Accounts and access to the network may not be managed, monitored, and authenticated using principles of least privilege or multifactor authentication. The MRE system end users may also have a small number of staff members responsible for cybersecurity, or the responsible staff members may have multiple responsibilities within the organization. The consequence of a cyberattack on the MRE system may have a significant impact on the end user's business (financial) or mission (operation) by affecting or failing the MRE system's function.

  Cybersecurity guidance will involve security measures required for Risk Level 2 and additional security measures to enhance physical and environment security, system testing, incident analysis, and assessment of security alerts and new threats.

## 4.2 Risk-Based Cybersecurity Best Practices

The MRE cybersecurity best practices were developed based on reviewing the mitigation strategies recommended by Dragos, MITRE ATT&CK Matrices, NIST CSF, NIST SPs, and ESCSWG. The resultant methods to protect MRE systems from a cyberattack follow the core functions described in the NIST CSF (e.g., identify, protect, detect, respond, and recover) and insights from security protection of information systems and ICS. Eighty-six security measures were identified and are grouped into the following nine categories:

- Account and Access Management (AC)
- Asset Management (AM)
- Communications Management (CM)
- Incident Preparedness (IP)
- Network Architecture and Security (NA)
- Physical and Environment Security (PE)
- Cybersecurity Program Management (PM)
- Cybersecurity Risk Management (RM)
- Security Development Practices (SD)

The language used to describe the best practices was taken from information on MRE system designs, configurations, and insights from one or more of the resource documents, such as NIST CSF, NIST SP 800-53, ESCSWG, and NERC CIP standards, in order to continue using standard industry terminology. Appendix D includes the summary overview of cybersecurity best practices that are recommended for the different risk levels (1,2, or 3). These best practices can also be implemented to supplement the cybersecurity requirements governed by the authoritative organization and from other specific security resource documents listed in Appendix D.

### 4.2.1 Account and Access Management

MRE system developers and operators must verify that the accounts, credentials, and sessions used to access either the MRE system itself or devices connected to the MRE system are properly secured and managed. Besides ensuring only authorized individuals are using accounts, other management methods include account configuration, implementing the principal of least privilege, and understanding and managing the sessions currently connected to the device. The following are the best practices in this category:

**AC.1:** Account Management. MRE systems, when initially manufactured, may be configured with default accounts and passwords that may be publicly available. Accounts used by developers to manage the system can be compromised by malicious actors by gaining unauthorized access to systems or to escalate privileges. This provides one of the easiest ways for an attacker to compromise a system. The tenets of AC.1 can be met by implementing the following measures:

> AC.1(1) *Manage Accounts*: Issue, manage, verify, revoke, and audit identities and credentials for authorized devices (including mobile and remote devices), users, and processes. Change default accounts to settings customized for the MRE system and remove or disable any accounts not needed for normal operations or maintenance or emergency operations of the MRE system. Maintain an up-to-date record of all active accounts.
>
> AC.1(2) *Configuration of Accounts*: Place all accounts for emergency operations in a highly secure configuration.

**AC.2:** Access Management. To prevent adversaries from unauthorized or undetected access to specific information systems, control systems, data/information, functions, software applications, locations, components, or resources, access control methods should be implemented. Unauthorized access to accounts that are created for use in the MRE system can be exploited by attackers to gain elevated permissions and either cause further damage or embed themselves deeper into compromised systems. Managing access control limits individual users and processes to accounts and processes by implementing the "principles of least privilege" and “separation of duties,” so that every process, program, or user is only authorized to access specific information and processes. Access control can also be managed by implementing multifactor authentication methods and managing passwords. The tenets of AC.2 can be met by implementing the following measures:

> AC.2(1) *Least Privilege and Separation of Duties*: Manage access permissions and authorizations by incorporating the principles of least privilege, separation of duties, bound to credentials, and asserted in interactions.
>
> AC.2(2) *Authentication*: Implement standards-based authentication and authorization protocols for users, devices, and other assets, such as multifactor authentication, password management, limiting the number of unsuccessful login attempts, and notifications of access.
>
> AC.2(3) *Access Protocols*: Restrict the transmission or sharing of user credentials in clear text and only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Termination Emulation, Transport Layer Security).

**AC.3:** Session Management. Remote access of the MRE system typically involves creating sessions for network access. Weak or insecure system session operating practices can result in vulnerabilities. These sessions, if not properly monitored and managed, can be hijacked or manipulated by attackers to gain or deny access to a system. The tenets of AC.3 can be met by implementing the following measures:

> AC.3(1) *Restrict Multiple Concurrent Logins*: Restrict multiple concurrent logins using the same authentication credentials and do not allow applications to retain login information between sessions, enable auto-fill functionality during login, and have anonymous logins.
>
> AC.3(2) *Session Termination:* Provide account-based and group-based configurable session-based logout and timeout settings (e.g., alarms and human-machine interface).
>
> AC.3(3) *Encryption, Digital Signing*: Provide appropriate level of protection for user credentials (i.e., restrict use of clear text), access protocols (i.e., encrypt or secure transmissions), and sessions (i.e., encrypt and digital signing) commensurate with the technology platform, communications characteristics, and response time constraints.

### 4.2.2 Asset Management

Threats to the MRE system depend entirely on the type of assets being used within it. These assets include physical hardware, software, data, and human resources. Without knowing what assets make up the MRE system, an organization cannot accurately assess the types of threats that would apply. Managing the assets under the organization's control includes taking inventory of existing and future systems, classifying those assets and categorizing them, managing the configuration of the assets to verify proper mitigations are in place, managing the organization’s information and data, and managing the organization's staff members who deal with the MRE systems.

The following are the requirements and sub-requirements in this category:

**AM.1:** MRE Assets Inventory. Critical to the risk management process is the categorization and inventory of the assets being protected. Within cybersecurity management, the first step usually involves identifying what the "crown jewels" of the system are, so that way the defensive perimeter can be designed to secure the most critical assets. To accomplish this task, steps must be taken such as conducting an Asset Inventory. The tenets of AM.1 can be met by implementing the following measures:

> AM.1(1) *Asset Inventory*: Develop a current inventory of MRE system assets, including physical devices and systems (including external systems), software platforms and applications and identify the resources based on their mission and business value.
>
> AM.1(2) *Manage Assets*: Manage assets throughout the life cycle of the MRE system (i.e., removal, transfers, and disposition).
>
> AM.1(3) *Maintenance of Assets*: Maintenance activities, such as inspecting, testing, maintaining, and repairing assets and systems as required by the vendor using approved and controlled tools. Maintenance activities (remote or local) should be approved, logged, and performed in a manner that prevents unauthorized access.

**AM.2:** Classification and Categorization. Understanding and categorizing the different types of assets within the MRE system allows management to make more informed decisions based on the asset criticality and overall value. The tenets of AM.2 can be met by implementing the following measures:

> AM.2(1) *Classify and Categorize MRE Assets*: Prioritize assets (e.g., hardware, devices data time, personnel, and software) based on their classification, criticality, and business value.

**AM.3:** Configuration Management. Configuration management focuses on establishing and maintaining consistency of a product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life. Maintaining consistency allows incidents to be detected and responded to more easily within the cyber domain. The tenets of AM.3 can be met by implementing the following measures:

> AM.3(1) *Configuration Baseline*: Create and maintain a baseline configuration of information technology and ICS, including communications and connectivity-related aspects, which will serve as future builds, releases, and/or changes to the IT/OT systems over the life cycle of the MRE system.
>
> AM.3(2) *Configuration Management Process*: Provide a process for managing and controlling configuration changes, such as baseline settings and component inventories; development, test, and operational environments; and procedures for developing, releasing, and updating key documentation.
>
> AM.3(3) *Life Cycle Security*: Maintain the cyber resilience of the MRE system throughout its life cycle starting from design, development, manufacture, storage, delivery, construction, implementation, acceptance testing, operations, maintenance, and decommissioning to

disposal by implementing a quality assurance program and validating that the software and firmware have undergone quality control testing to identify and correct cybersecurity weaknesses and vulnerabilities.

AM.3(4) *Manage Data Environment:* Segregate the development and testing environments from production environment to eliminate impact.

AM.3(5) *Integrity Checks*: Verify integrity of firmware, hardware, and software by implementing checking mechanisms.

AM.3(6) *Backup of Information*: Implement methods to back up data and information (i.e., log files, databases, programs, log files, etc.) and implement security measures to prevent unauthorized access and modification; backup files should be maintained and tested to verify integrity of data.

**AM.4:** Information and Data Security. Information and data are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. This approach includes both in transit and when at rest and considers the flow of the data through different systems and machines. The tenets of AM.4 can be met by implementing the following measures:

AM.4(1) *Data Flow*: Identify and map the MRE system and organization's data flow and communications, including CUI (i.e., sensitive data, business-sensitive data, MRE system emergency operation procedures, drawings, security information, etc.).

AM.4(2) *Protect Confidentiality, Integrity, and Availability of Data*: Protect information and data at rest, in transit, and stored to verify its integrity, availability, and confidentiality by making sure there is adequate data capacity and preventing unauthorized disclosure, leaks, loss, or manipulation of information or data.

AM.4(3) *Maintenance of Data Protection Processes*: Continuously review and improve the effectiveness of data protection processes through periodic evaluation.

AM.4(4) *Destruction of Data*: Develop a process for properly sanitizing MRE system data (i.e., design, as-built drawings, emergency procedures, interconnection agreements, security plan information, etc.) prior to disposal or release outside of the organization's control, so that it cannot be retrieved or reconstructed.

AM.4(4) Protection of CUI: Protect CUI using guidance provided in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

**AM.5:** Personnel Security. Personnel that have access to the MRE system (e.g., organization's staff, temporary vendors, contractors, third-party personnel) are protected and managed effectively to make sure that single point of failure does not exist as a result of staffing. The tenets of AM.5 can be met by implementing the following measures:

AM.5(1) *Personnel Protection*: Incorporate cybersecurity practices into management of organization's staff, including temporary staff, contractors, and third-party personnel that have direct access to the MRE system and its networks, which will include designating security risk positions, performing background checks, and securing access privileges upon termination or transfer of duties.

AM.5(2) *Monitor Personnel Activity*: Monitor personnel activity to detect potential cybersecurity events, unauthorized personnel access, connections, devices, and software.

### 4.2.3 Communications Management

The network architecture for MRE systems may have a variety of communication methods. Implementing appropriate security controls to protect the methods that an MRE system uses to communicate data and control systems will provide assurance of the confidentiality, integrity, and availability of that communication.

The following are the requirements and sub-requirements in this category:

**CM.1:** Organizational Communication. Along the lines of network design, mapping the organizational structure of the communications within the MRE system helps identify outliers and rogue devices. With an established map in place, MRE administrators can detect devices and communication protocols that are out of the ordinary on the network with much more speed and accuracy. The tenets of CM.1 can be met by implementing the following measures:

CM.1(1) *Communication Mapping*: Map the communication methods (e.g., protocols) and data flow between systems or components, including remote access capabilities, and between network security zones (inbound and outbound).

CM.1(2) *Communication Restrictions*: Provide and document methods used to restrict communication traffic between different network security zones and verify that disconnection points are established between network security zones.

**CM.2:** Wireless. MRE systems may use wireless technologies that bypass physical access and typical permissions associated with physical access. Wireless technology should be protected to mitigate the threat of the wireless network being used by individuals without the organization's knowledge or consent. The tenets of CM.2 can be met by implementing the following measures:

CM.2(1) *Wireless Communication Protocols*. Document specific protocols (i.e., power and frequency requirements, range limitations), access controls and encryption, and other detailed information required for wireless devices to communicate with the control network, including other wireless equipment that can communicate with the MRE system devices. Security protocols shall comply with standard operational and security requirements specified in applicable wireless standards or specifications (e.g., applicable IEEE standards, such as 802.11 and guidance from NIST SP 800-48, NIST SP 800-97).

CM.2(2) *Wireless Use Restrictions*: Document use, capabilities, and limits for the wireless devices and demonstrate through test data that known attacks (e.g., those documented in the Common Attack Pattern Enumeration and Classification list, such as malformed packet injection, man-in-the middle attacks, or denial of service attacks) do not cause MRE system wireless devices to crash, hang, be compromised, or otherwise malfunction.

CM.2(3) *Network Rules Between Wireless and Wired*: Establish configuration settings for network components to restrict or limit wireless access points in order to protect the information system from external and internal wireless communication links.

**CM.3:** Remote Access. MRE systems are expected to be located in ocean waters that are away from coastal communities and facilities. As such, MRE systems may be accessed remotely by a developer or engineer (e.g., MRE system owner, vendor, or third-party partner) for monitoring, maintenance, or improvements/updates. Vulnerabilities and threats are associated with different methods of remote access (i.e., local area network, wide area network, Cloud, etc.). Within the energy industry, this remote access functionality is one of the primary targets for threat actors. For this reason, mitigation strategies for remote access are critical to the overall cybersecurity posture of the MRE system. The tenets of CM.3 can be met by implementing the following measures:

> CM.3(1) *Managed Devices*: Document all remote access entry pathways and make sure they can be enabled or disabled by MRE owner as needed.
>
> CM.3(2) V*irtual Private Network, Bastion Host*: Provide methods, such as communication tunneling (e.g., a virtual private network) to support communications with any remote system or network and maintain a security-isolated environment outside the control network (e.g., using a demilitarized zone or an equivalent or a superior form of security isolation) for the communications tunneling server to reside.
>
> CM.3(3) *Usage Restrictions*: Establish and document usage restrictions and configuration/connection requirements for each type of remote access for authorized remote access users.

**CM.4:** Encryption. Encryption makes sure that both the confidentiality and integrity of data within the MRE System remain intact. With improper configuration or unsecured methods, encryption can be compromised and confidentiality, integrity, and/or availability can be compromised as well. A cryptographic-based security system includes both cryptographic methods and cryptographic key management. The tenets of CM.4 can be met by implementing the following measures:

> CM.4(1) *Cryptographic System Documentation*: Establish a baseline set of documentation detailing which cryptographic primitives (e.g., algorithms) will be implemented for the MRE system and how those primitives will be implemented and managed throughout the life cycle of the MRE system.
>
> CM.4(2) *Manage Cryptographic Key*: Manage cryptographic keys by identifying the policy for creating, distributing, maintaining, validating, and updating cryptographic keys and provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

### 4.2.4 Incident Preparedness

A cybersecurity program not only identifies assets, protects the assets, and detects potential security vulnerabilities but also prepares to respond and recover from a potential cyberattack. To prepare for a cyber incident, the organization should develop a plan that identifies roles and responsibilities during an incident, the communications between the different roles and responsibilities, and recovery of information and business operation after a cyber incident.

The following are the requirements and sub-requirements in this category:

**IP.1:** Incident Preparedness Policy. Remote access of the MRE system typically involves creating sessions for network access. Weak or insecure system session operating practices can result in vulnerabilities. MRE organizations should define incident preparedness policies and procedures that guide the response activities as an essential step to establishing an incident response capability to protect MRE assets. Incident preparedness policies, including suppliers and third-party partners, should cover additional activities, including assigning responsibilities to individuals, providing appropriate training and awareness, formalizing information flows, and selecting, installing, and understanding the tools used in the response effort. Management should define thresholds for reporting significant security incidents and consider developing processes for when the MRE organization should notify its regulators of incidents that may affect the institution's operations, reputation, or sensitive customer information. The tenets of IP.1 can be met by implementing the following measures:

IP.1(1) *Incident Preparedness Policy*: Develop the organization's policy to prepare for a cybersecurity incident. The policy should, at a minimum, describe the following:

- Essential missions and business priorities that are to be maintained during the incident and recovered after the incident
- Recovery objectives, restoration priorities, and metrics
- Makeup of an Incident Response Team (IRT)
- Training and awareness program for IRT
- Methods of communication between IRT members
- Reporting of the incident to internal and external organizations
- Response and contingency plan to recover data and essential mission and business functions despite the interruption, compromise, or failure of the systems

IP.1(2) *Incident Preparedness with Suppliers and Third-Party Partners*: Conduct response and recovery planning with suppliers and third-party providers.

**IP.2:** Incident Response. Incident detection and response plans, procedures, and methods are necessary for rapidly detecting incidents, performing incident analysis, minimizing loss and destruction, preserving evidence for later forensic examination, mitigating the weaknesses that were exploited, and restoring ICS services. Establishing a successful incident response capability includes continually monitoring for anomalies, prioritizing the handling of incidents, and implementing effective methods of collecting, analyzing, and reporting data. MRE organizations should verify that personnel are provided appropriate training and awareness to carry out Incident Response Plan roles and responsibilities. Additionally, MRE organizations should periodically review and update the cybersecurity Incident Response Plan. The tenets of IP.2 can be met by implementing the following measures:

IP.2(1) *Incident Response Plan*: Design and develop a plan to respond to a cybersecurity incident and the methods to protect systems and assets. The plan should include the following:

- Roles and responsibilities of an IRT, which should comprise individuals from different organizations, such as security, operations, engineering, emergency preparedness, and other support personnel, as appropriate
- Methods of coordinating and communicating with internal and external organizations
- Process to facilitate and maintain the continuity of operations of assets and systems by containing and mitigating the incident

IP.2(2) *Incident Response Team Training*: Develop a training and awareness program for the IRT to make sure appropriate personnel, including contractors and sub-contractors, are aware of the cybersecurity best practices and are knowledgeable in the actions to take in response to a cybersecurity incident. The training and awareness program should define the roles and responsibilities for the IRT, methods of communication between IRT members and external organizations, and performance of a cyber-incident exercise.

IP.2(3) *Periodic Review and Update of Incident Response Plan*: Review and update the organization’s Cybersecurity Response Plan to make sure the response strategies continue to be effective and incorporate lessons learned during an actual cyber incident or a planned exercise.

IP.2(4) *Incident Analysis*: Conduct and document an analysis of the organization's response to an incident (actual or exercise) to understand the impact of the incident, perform forensics, identify new vulnerabilities and mitigating strategies, and categorize the incident in accordance with the response plan.

**IP.3:** Incident Recovery. To have business continuity for the MRE system and end user after a cyber incident, a recovery plan is developed to describe methods to restore systems from known valid backups, separating systems from all non-essential interferences and connections that could permit cybersecurity intrusions, and alternatives to achieve necessary interfaces and coordination. The recovery plans should be periodically reviewed with employees responsible for restoration of the ICS and tested to make sure that they continue to meet their objectives. The tenets of IP.3 can be met by implementing the following measures:

IP.3(1) *Recovery Plan*: Develop a Cybersecurity Recovery Plan to restore systems and assets affected by a cyber incident. The recovery plan should describe the following:

- Roles and responsibilities within the organization
- Strategies to restore systems and assets to provide continued stability, operability, and reliability of the MRE system
- Methods of communicating the restoration activities between internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of systems and assets, vendors, etc.)
- Contingency plan to recover data from designated backup storage and essential mission and business functions if interruption, compromise, or failure of the assets or systems occurs

IP.3(2) *Review and Update Recovery Plan*: Review and update the organization’s Cybersecurity Recover Plan to make sure the recovery strategies continue to be effective and incorporate lessons learned during an actual cyber incident or a planned exercise.

IP.3(3) *Recovery Plan Training and Awareness*: At least once a year, validate the effectiveness of the organization's recovery plan and methods by performing a paper drill (tabletop exercise) or hands-on drill (operation exercise). A critique of the training exercise should be performed to identify best practices and opportunities for improvement (lessons learned).

**IP.4:** Incident Reporting. Reporting cybersecurity incidents is a requirement for MRE systems that are used by federal agencies and their subordinate organizations. The intent of reporting incidents is to enable incidents to be integrated in a centralized location, including the operational elements involved in cybersecurity and communications reliance. The tenets of IP.4 can be met by implementing the following measures:

IP.4(1) *Incident Reporting Policy*: Develop the organization's policy for reporting cybersecurity incidents internal to the organization (senior management) and external (e.g., required reporting to federal agencies and their subordinate organizations). The policy should include documenting the incident, providing descriptions of types of incidents to report, enabling the content and timeliness of reports, and identifying the designated authorities to report incidents.

### 4.2.5 Network Architecture and Security

Poorly designed network architectures that lack a defense-in-depth approach to security may be vulnerable to cyber exploitation. Security can be enhanced by partitioning networks into multiple segments and placing technical security controls (e.g., firewalls, unidirectional communication devices, or virtual private network concentrators) between the network segments. Hardware, software, and firmware that restrict communications are important tools in establishing an appropriate cybersecurity defensive architecture. The network architecture is how a network is designed and segmented into logical, smaller functional subnets (i.e., network security zones) for the purpose of communication.

The following are the requirements and sub-requirements in this category:

**NA.1:** Network Design. The overall design of the network including the hierarchy schema and the flow of traffic directly correlates to how potential attacks will be carried out against the MRE system. Components to designing the network include how the network is configured, baseline measurements, firewalls, and data flows. The tenets of NA.1 can be met by implementing the following measures:

NA.1(1) *Design Baseline*: Establish and manage a baseline of network operations and expected data flows for different users and systems.

NA.1(2) *Least Functionality Configuration*: Incorporate the principle of least functionality when configuring the systems to provide only essential services and capabilities (i.e., network ports and protocols are functioning to complete core tasks).

NA.1(3) *Firewalls*: Provide firewalls and document rule sets for normal and emergency operation, including “deny all,” with exceptions identified by MRE System owner/operator.

**NA.2:** Network Protection. Protecting the network while operating it involves putting mitigation strategies in place from applicable threats to the MRE system. The tenets of NA.2 can be met by implementing the following measures:

NA.2(1) *Network Communications*: Protect control and communications networks by providing disconnection points between network security zones, restricting communication traffic between network security zones, and monitoring network traffic.

**NA.3:** Network Detection. Intrusion detection systems are used to detect an attempt to compromise the confidentiality, integrity, and availability of IT/OT systems paramount to the operation of the MRE system. The intrusion detection system can be an individual hardware component or specialized software that monitors the network or system activities for malicious activities or policy violations and logs or reports potential issues. The tenets of NA.3 can be met by implementing the following measures:

NA.3(1) *Detection*: Establish and manage a method to detect (i.e., host or intrusion detection systems), collect (i.e., auditing and logging), and analyze events from multiple sources and sensors to understand the attack targets, methods, and impact of events.

NA.3(2) *Alerts*: Establish incident alert thresholds.

**NA.4:** Network Monitoring. Critical to catching network intruders in a timely manner involves actively monitoring the network and the ability to classify traffic as malicious or benign. Through the use of environment monitoring, security information and event management, and malware detection strategies, an organization can classify an incident as a threat quickly and efficiently. From there, proper communication of the detected incidents ensures the information is used to effectively to mitigate attacks on the MRE systems. The tenets of NA.4 can be met by implementing the following measures:

NA.4(1) *Security Information and Event Management*: Monitor and track (i.e., audit) the network to detect potential cybersecurity events, such as unauthorized access, changes to configuration of information systems, access system boundary, or external service provider activity.

NA.4(2) *Malware Detection*: Detect malicious code (e.g., malware) and unauthorized mobile codes by providing methods to detect host-based malware by scanning systems, including emails and websites, and removable media that are introduced to the MRE system. The host-based malware detection capability shall also test and confirm compatibility of malware detection application patches and upgrades.

NA.4(3) *Communicate Event Detection*: Provide a method to communicate detection of events.

**NA.5:** Auditing. Recording specific system activity in the form of logging generates an audit trail. Failure to perform logging makes it difficult to monitor activity, identify potential cyberattacks in time to take protective actions, perform diagnostics, and carry out forensic activities if a successful cyberattack occurs. Without easy access to information on system activity, post-event investigations may not yield conclusive results, and the risk of similar events occurring in the future would remain high. The tenets of NA.5 can be met by implementing the following measures:

NA.5(1) *Audit/Log Events*: Audit/log records are generated, time-stamped, and documented to cover the following activities:

- Account usage, including remote access
- Wireless and mobile device connectivity
- Configuration settings and changes
- System component inventory (install and removal)
- Communications at information system boundaries
- Use of maintenance tools and non-local (remote) maintenance
- Physical access
- Environmental conditions and changes (temperature and humidity)
- Use of mobile code and Voice over Internet Protocols

NA.5(2) *Audit/Log Records*: Audit/log records should be managed using a Security Information and Event Management integration method, stored (e.g., transfer or log forwarding), and maintained.

NA.5(3) *Audit Review, Analysis, Reporting*: Review, analyze, and report audit/log records of monitoring activities incidents (attempted or successful) to perform diagnostics or conduct forensic activities if a successful cyberattack occurs.

### 4.2.6 Physical and Environment Security

Protecting against methods of physical impact to the system's environment is paramount to the cybersecurity of the system. Allowing malicious actors to physical access the device can be immediately catastrophic in multiple ways and forms. In addition, the devices that are ultimately attached or connected to the MRE system, even by an authorized user, can inadvertently do critical damage to both the security posture and the operation of the MRE system. Depending on the location of the MRE system itself, physical access can be easier or more difficult. In situations where an attacker could easily access the system, more physical security measures are needed. Certain design and operation techniques, such as limiting removable media, reducing wireless leakage, and creating a robust physical perimeter, can make it adequately difficult for an attacker to compromise or disrupt the system.

The following are the requirements and sub-requirements in this category:

**PE.1:** Physical Security. Physical security is an important element in cyber defense for MRE systems. Physical security is used to deter, delay, detect, and deny physical access by unauthorized individuals, including those who may wish to physically access energy-delivery system components to compromise the confidentiality, integrity, or availability of the systems or their data. The tenets of PE.1 can be met by implementing the following measures:

PE.1(1) *Manage Access to Assets*: Provide perimeter access security and physical security to the MRE system from manipulation, sabotage, or theft. Physical access to the perimeter boundary and the MRE system shall be managed and protected by controlling the authorization of personnel (i.e., staff, contractors, vendors, and visitors) and providing lockable or locking enclosures to the MRE system, system components (i.e., servers, networking hardware, supervisory control and data acquisition systems, etc.) and the systems that manage and control physical access (i.e., servers, lock controllers, alarm control panels, etc.).

**PE.2:** Manage Media. Within the marine industry specifically, the use of removable media to compromise remote and critical systems has had extremely effective results. It is important to have policies and configurations in place to limit and restrict the use of removable media on systems designed to function on the water to specifically combat malicious hackers. The tenets of PE.2 can be met by implementing the following measures:

PE.2(1) *Removable Media*: Protect the MRE system network by protecting and restricting the use of removable media, such as digital media (i.e., diskettes, magnetic tapes, externa/removable hard disk drives, flash drives, compact disks, digital video disks, etc.) or non-digital media (i.e., documentation, microfilm, etc.).

**PE.3:** Data Leakage. The methods used to transport data to and from the MRE system leave them open to sniffing (or eavesdropping). In a more serious scenario, an attacker that has access to the medium that is transporting data can execute a man-in-the-middle attack, controlling and spying on traffic going both to and from a particular point. While wireless networks are particularly vulnerable to information leakage, wired networks too can become susceptible, albeit at a much closer range. However, wireless and wired design principles can be followed that can dramatically reduce both the amount and range of data leakage from the MRE system. The tenets of PE.3 can be met by implementing the following measures:

> PE.3(1) *Wireless Leakage*: Implement appropriate methods and design elements to prevent the leak of wireless communication outside of the physical security controls provided to protect MRE systems, such as auditing the range of the wireless networks, implementing techniques to reduce transmission range, and aiming any sending/receiving antenna in the correct direction.
>
> PE.3(2) *Physical Leakage*: Implement appropriate methods and design elements to prevent wired communication or interconnections to the MRE system from leaking beyond the physical security controls.

**PE.4:** <u>Environment Management</u>. Management information systems and the environments in which those systems operate protect the MRE systems from adversaries by not giving them sufficient time to target and exploit vulnerabilities. The tenets of PE.4 can be met by implementing the following measures:

> PE.4(1) *Manage Environment*: Implement and monitor the development, testing, and physical and operating environments of the MRE system to detect potential security events.
>
> PE.4(2) *Monitor Physical Environment*: Monitor and track (i.e., audit) the physical environment to detect potential cybersecurity events by providing tamper detection or locking enclosures. Re-programming of locking code and changes to locks, keycards, and other keyed entrances should be performed periodically.

### 4.2.7 Cybersecurity Program Management

A cybersecurity program provides a roadmap of the security management practices and organization-defined common controls to protect the MRE system from cyber threats. The program can be represented in a single document or a compilation of documents at the discretion of the MRE system owner. At a minimum, the cybersecurity program includes a description of the roles and responsibilities of personnel necessary to implement the programmatic requirements (e.g., development, implementation, assessment, authorization, and monitoring of security controls), the applicable legal and regulatory requirements to make sure the cybersecurity program is developed commensurate with the risk of a cyberattack, a plan that describes the program requirements and security controls, a description of the associated policies and procedures, and the necessary awareness and training required for the organization to communicate and implement the cybersecurity best practices.

The following are the requirements and sub-requirements in this category:

**PM.1:** <u>Cybersecurity plan</u>. A cybersecurity plan documents the organization's Cybersecurity Program and is the method used to communicate, at a high level, how the MRE system meets the cybersecurity best practices without providing details and technical description of the design and security controls that are implemented. The cybersecurity plan is expected to be periodically reviewed and updated to remain current. The tenets of PM.1 can be met by implementing the following measures:

PM.1(1) *Cybersecurity Plan*: Develop, document, review, and update a cybersecurity plan that describes the Cybersecurity Program requirements, a general description of the security controls that implement the requirements, the organization that manages the cybersecurity program, including roles and responsibilities, the governance and risk management processes, and the implementing procedure and/or instructions.

PM.1(2) *Maintenance of Cybersecurity Plan*: Develop a process to review changes to the MRE system design, operations, and configuration and evaluate the impact on the cybersecurity plan commensurate with the MRE systems risk.

**PM.2:** Cybersecurity Organization. Paramount to the security of energy systems is the assignment of individuals in an organization that perform certain security-relevant functions that are different from other members of the organization's staff. The designation of staff dedicated to cyber-specific roles also provides accountability for specific aspects of the organization's cybersecurity program and will be the basis for authorizing access and privileged roles. The tenets of PM.2 can be met by implementing the following measures:

PM.2(1) *Roles and Responsibilities*: Identify specific roles and responsibilities for the organization and third-party stakeholders (i.e., suppliers, customers, partners), such as designating officials for chief information system officer, organizational risk executive, and other roles and responsibilities described in NIST SP 800-37.

**PM.3:** Cybersecurity Governance. The cybersecurity for the MRE system is governed by the regulations that dictate the protection of the end user. The legal guidelines are based on the use of the MRE system, which directly informs what kinds of security controls the system must have to be at an acceptable level of security. The tenets of PM.3 can be met by implementing the following measures:

PM.3(1) *Legal and Regulatory*: Identify legal and regulatory environments that would be enforceable for the MRE system and its mission (i.e., NERC CIPs, DoD, etc.), including communications and reporting of cyber incidents.

**PM.4:** Cybersecurity Policies and Procedures. Specific policies and procedures relating to the organization's overarching cybersecurity plan should be properly defined and implemented to produce the best results for improving the security posture. The tenets of PM.4 can be met by implementing the following measures:

PM.4(1) *Policies and Procedures*: Identify, document, and disseminate policies for aspects of the cybersecurity program requirements, such as Risk Management and Supply Chain Risk Management, including periodic review and updates. The policy and process should address purpose, scope, roles, responsibilities, management commitment, coordination with other organization entities, and compliance. Procedures should also be developed to facilitate implementation of the policy and controls for compliance.

**PM.5:** Awareness and Training. Training is overwhelmingly the #1 recommended mitigation strategy for reducing cyber incidents in any system. Adequate training for staff at all levels of the organization can reduce the attack surface dramatically. The tenets of PM.5 can be met by implementing the following measures:

PM.5(1) *Training:* Develop a training program to educate the organization's personnel (senior executives, security staff (physical and cyber), general users, and privileged users) and partners (vendors, contractors, sub-contractors, suppliers, etc.) on the cybersecurity program for the MRE system to understand their roles and responsibilities. The training should be provided prior to engaging with MRE system designs, operations, and maintenance, and at least annually thereafter.

PM.5(2) *Training Records*: Records of training for each staff member and partner will be maintained throughout the life cycle of the MRE system.

### 4.2.8 Cybersecurity Risk Management

An organization's risk management strategy outlines how the organization properly identifies, weighs, and mitigates risks posed to both the MRE system and the organization. The risk management strategy includes defining the organization's mission objective, identifying acceptable risk tolerance, implementing acceptable risk assessment methods, and identifying new or modifying existing risk mitigation strategies based on the guidance provided in applicable industry security standards for MRE systems. The risk management strategy extends to managing risks involving the MRE system supply chain.

The following are the requirements and sub-requirements in this category:

**RM.1:** Mission Security. MRE systems are designed to deliver reliable and secure energy for different markets. Knowing the mission/business functions for the MRE system and its end use will aid in implementing appropriate cybersecurity controls to protect assets and developing effective incident response and recovery strategies to achieve continuity of operations. The tenets of RM.1 can be met by implementing the following measures:

RM.1(1) *Cybersecurity Objectives and Goals*: Identify and document the MRE system's mission and business objectives that are to be protected from a cyberattack and the types of threats (both internal and external) and system vulnerabilities that could potentially affect these objectives. Identify and document the security measures that are implemented to mitigate the cybersecurity risks.

RM.1(2) *Business Environment*: Identify and communicate the MRE system's role in the critical infrastructure for the end user and the supply chain to inform the appropriate roles, responsibilities, and risk management decisions and establish resiliency requirements for the MRE system based on the organizational risk tolerance.

**RM.2:** Security Standards. Adherence to security standards is one step in protecting energy delivery systems and components from compromise. These standards should be considered when procuring energy delivery systems and components to improve security implementation, including the protection of sensitive information. The tenets of RM.2 can be met by implementing the following measures:

RM.2(1) *Reliance and Adherence to Standards*: Implement cybersecurity measures using current applicable interoperability and security standards, such as NIST SP 800-53, NIST SP 800-82, NIST SP 800-171, NERC CIP, etc. and comply with applicable requirements.

**RM.3:** Risk Assessments. To effectively manage cybersecurity, the MRE system operators need to understand their cybersecurity risks and validate the effectiveness of the security controls to protect the organization's assets. Risk-based cybersecurity management is a life cycle process that can be accomplished systematically and cost effectively and result in a substantial reduction in the likelihood of a successful cyberattack damaging expensive equipment or having a negative impact on the reputation of the organization. The tenets of RM.3 can be met by implementing the following measures:

RM.3(1) *Vulnerability Assessments*: Perform periodic vulnerability assessment of the MRE system assets to determine the MRE system’s cybersecurity risk commensurate with the MRE system owner's discretion. Document cybersecurity risk by identifying threats (internal and external), program vulnerability, and assessing the impact to the organization’s mission and business. These cybersecurity risks are the basis for the cybersecurity protection provided for the MRE system.

RM.3(2) *Vulnerability Management Plan*: Develop and implement a vulnerability management plan to include scanning for all information system components (i.e., patch levels, functions, ports, protocols, services, configuration, data flow, etc.), recording/logging of the scan, and the remediation phase (mitigating strategies).

RM.3(3) *Vulnerability Scanning:* Periodically scan for vulnerabilities in the information systems and hosted applications using standard tools and techniques.

RM.3(4) *Risk Assessment Process*: Periodically assess the MRE system's cybersecurity risk by evaluating threats, vulnerabilities, likelihoods, and impact on the MRE system operation and end user's mission and business and prioritizing risk mitigating strategies.

RM.3(5) *Plan of Action and Milestones*: Establish a process to identify plan of action and milestones to address gaps in cybersecurity practices to include system and network vulnerabilities, document remedial actions to address risk to organization operations and assets, individuals or other organizations, and periodically review plan of action and milestones for organization risk management strategy.

**RM.4:** Supply Chain Risk Management. Security breaches may also affect the cybersecurity of procured products. Such breaches may involve compromise of the supplier's organization or any organization involved in the product’s supply chain. Security breaches may result in loss of MRE system design information, use and configuration of the products, and compromise of access control information or other security and business-sensitive information. MRE system owners may be able to apply mitigating measures to maintain adequate levels of security if a security breach from its suppliers or third-party partners is known. The tenets of RM.4 can be met by implementing the following measures:

RM.4(1) *Supply Chain Risk Management Policy*: Identify, establish, assess, and manage a cybersecurity supply chain risk management process that is agreed to by MRE system owner and stakeholder and incorporate appropriate measures into contracts with suppliers and third-party vendors to meet the objectives of the Supply Chain Risk Management policy.

RM.4(2) *Suppliers and Third-Party Partners*: Identify suppliers and third-party partners of IT/OT systems, components (hardware, software, and firmware), and services and assess the suppliers' and partners’ security program using a cyber supply chain risk assessment process.

RM.4(3) *Delivery Protection*: Provide methods to secure the delivery of IT/OT systems, components and services from trusted channels (i.e., shipped through U.S. registered mail), including digital delivery using trusted means (encrypted). These protection methods shall be monitored throughout the delivery to detect unauthorized access, and receipt of the delivery shall be validated upon receipt.

RM.4(4) *Periodic Audits*: Assess suppliers and third-party partners using audits, test results, or other forms of evaluation to confirm they are meeting their contractual obligations.

### 4.2.9 Security Development Practices

As the MRE system is designed and developed, information security practices must be incorporated within the development cycle to minimize the number of vulnerabilities that are created and mitigate the vulnerabilities that do appear. This process includes conducting periodic security assessments on both the MRE system and the components that are working to create it. In addition, participating and complying with security alerts/advisory systems like those produced by US-CERT help keep the development team informed on known issues and vulnerabilities.

The following are the requirements and sub-requirements in this category:

**SD.1:** Security Assessments. To make sure that effectiveness of information security is built into the MRE system design and operations, an assessment of security controls implemented in the MRE information systems and operating environment(s) is performed periodically. The intent of the security assessment and security testing is to identify weakness and deficiencies during the life cycle of the MRE system (e.g., design, construction, operations, decommissioning, and disposing), provide information needed to make risk-based decisions, and verify compliance with the organization's cybersecurity program, policies, and procedures. The tenets of SD.1 can be met by implementing the following measures:

SD.1(1) *Periodic Security Assessments*: Conduct periodic security assessments (onsite and tabletop) of the MRE system by an independent third party.

SD.1(2) *Security Testing*: Implement methods to test the security of the IT-based network.

**SD.2:** Security Alerts, Advisories, and Directives. US-CERT generates security alerts and advisories to maintain situational awareness, and the Office of Management and Budget issues security directives. Compliance with the security directives is essential due to the critical nature and the potential immediate adverse effects on MRE system operations and assets, individuals, other organizations (i.e., supply chain partners, external mission/business partners, external service providers, etc.), and the nation. The tenets of SD.2 can be met by implementing the following measures:

SD.2(1) *Security Alerts*: Receive information system security alerts, advisories, and directives on an ongoing basis, disseminate to appropriate personnel in the organization, and implement recommendations within the recommended time frames. Generate internal security alerts, advisories, and directives, as deemed necessary.

SD.2(2) *Threat intelligence*: Receive cyber-threat intelligence from information-sharing forums and resources and process the threat intelligence to determine impact on risk.

## 4.3 Implementation of Security Program and Assess Controls

After the MRE system owner/operator selects the appropriate best practices commensurate with the risk level of the IT/OT systems, the security program can be developed and implemented. Step 3 of the MRE System RMF (Figure 6) implements the security program and assesses the security controls. Documentation of the policies and security measures that are implemented on the MRE systems are included in a Cybersecurity Plan. Other policies, such as Incident

Preparedness, Supply Chain Risk Management, Risk Management, etc., are also developed at this stage prior to deployment and commissioning of the MRE system.

## 4.4 Deployment of the MRE System

The cyber resilience and reliability of the MRE system are important prior to connection of the energy-generating asset to the stakeholder. In Step 4 of the MRE System RMF (Figure 6), the MRE system is ready to be deployed and commissioned after construction of the MRE system, implementation of security measures, and development of the Cybersecurity Program (i.e., roles and responsibilities, policies and procedures, training, etc.). The process for deploying the MRE system is governed by the stakeholder.

## 4.5 Periodic Risk Assessments

To measure the effectiveness of the cybersecurity measures and the program policies and procedures, it is important to perform periodic risk assessments. The frequency to perform the risk assessments is generally once a year, but it may need to be done more frequently based on the stakeholder's needs. Implementation of a risk assessment would follow best practices for RM.3 developed from NIST and other guidance (see section 4.2 of this report). The risk assessment [RM.3(3)] may also include performing vulnerability assessments, [RM.3(1)]. Important to note is the development of a plan of action and milestones [RM.3(5)] that identifies gaps in implementation of the Cybersecurity Program and practices, including vulnerabilities of the system and network. The plan of action and milestones also provides the stakeholder an opportunity to develop remedial actions to address the risk to organization operations and assets, individuals, or other organizations. The plan of action and milestones is periodically reviewed to validate the effectiveness of the organization's risk management strategy.

## 4.6 Continuous Monitoring

It is necessary to continuously monitor the security of the MRE IT/OT systems to detect any attempts to connect to or access the network. This process, Step 6 of the MRE system RMF, involves development of a monitoring strategy, which includes developing metrics to measure acceptability/effectiveness of the program's security measures and identifying thresholds of actions that need to be taken if an incident occurs. As part of continuous monitoring, data is collected, analyzed, and reported to provide an audit trail of information if an incident occurs. The strategy developed to continuously monitor the security of the MRE system is also periodically reviewed and updated, as appropriate. In some cases, the MRE system stakeholder may want to obtain results of the performance and health of the cybersecurity program. The data obtained from continuously monitoring the systems would either be sufficient to demonstrate the effectiveness of the security measures implemented or identify the need to improve existing security measures.

## 4.7 Implementation of the Risk Management Framework

As shown in Figure 6, the MRE System RMF is a continuous cycle. When IT/OT assets are modified or replaced, the initial steps of identifying the risks, implementing security controls, deploying the modified asset, performing risk assessments, and monitoring the security of the MRE system will continue throughout the life cycle of the energy-generating system.

# 5.0 Conclusion

The advanced IT/OT used in MRE system designs provides a cyberattack surface to gain unauthorized access to data or disrupt operation of the energy-generating device. This report describes a framework for managing the cybersecurity risks of an MRE system. The six-step process in the MRE system RMF provides guidance on continuously identifying threats, implementing security measures, and monitoring the effectiveness of the cybersecurity program. This report also identifies best practices that were tailored to protect the IT/OT systems inherent in MRE devices commensurate with the risk from a cyberattack. The security best practices are developed using insights from the core functions of the NIST CSF,  NIST SP 800-53, NIST SP 800-82, ESCSWG report, NERC CIP Reliability Standards, and existing cybersecurity guidance for the maritime industry. Figure 6 summarizes the 86 cybersecurity best practices developed to protect MRE systems, which are grouped into the following nine categories:

- Account and Access Management
- Asset Management
- Communications Management
- Incident Preparedness
- Network Architecture and Security
- Physical and Environment Security
- Cybersecurity Program Management
- Cybersecurity Risk Management
- Security Development Practices

In Figure 7, the best practices are also color-coded to the core functions of the NIST CSF (e.g., identify, protect, detect, respond, and recover). MRE system developers, owners, and operators can implement the cybersecurity best practices commensurate with the cybersecurity risk of the device, their operational configuration, and the authoritative cybersecurity governance. The cybersecurity best practices are continuously reviewed and will be updated as the maturity of the MRE system designs grows and more information on the IT/OT configurations and operational processes is available. These best practices were developed from the initial input of IT/OT assets provided by MRE developers and the limited information available on currently deployed MRE systems

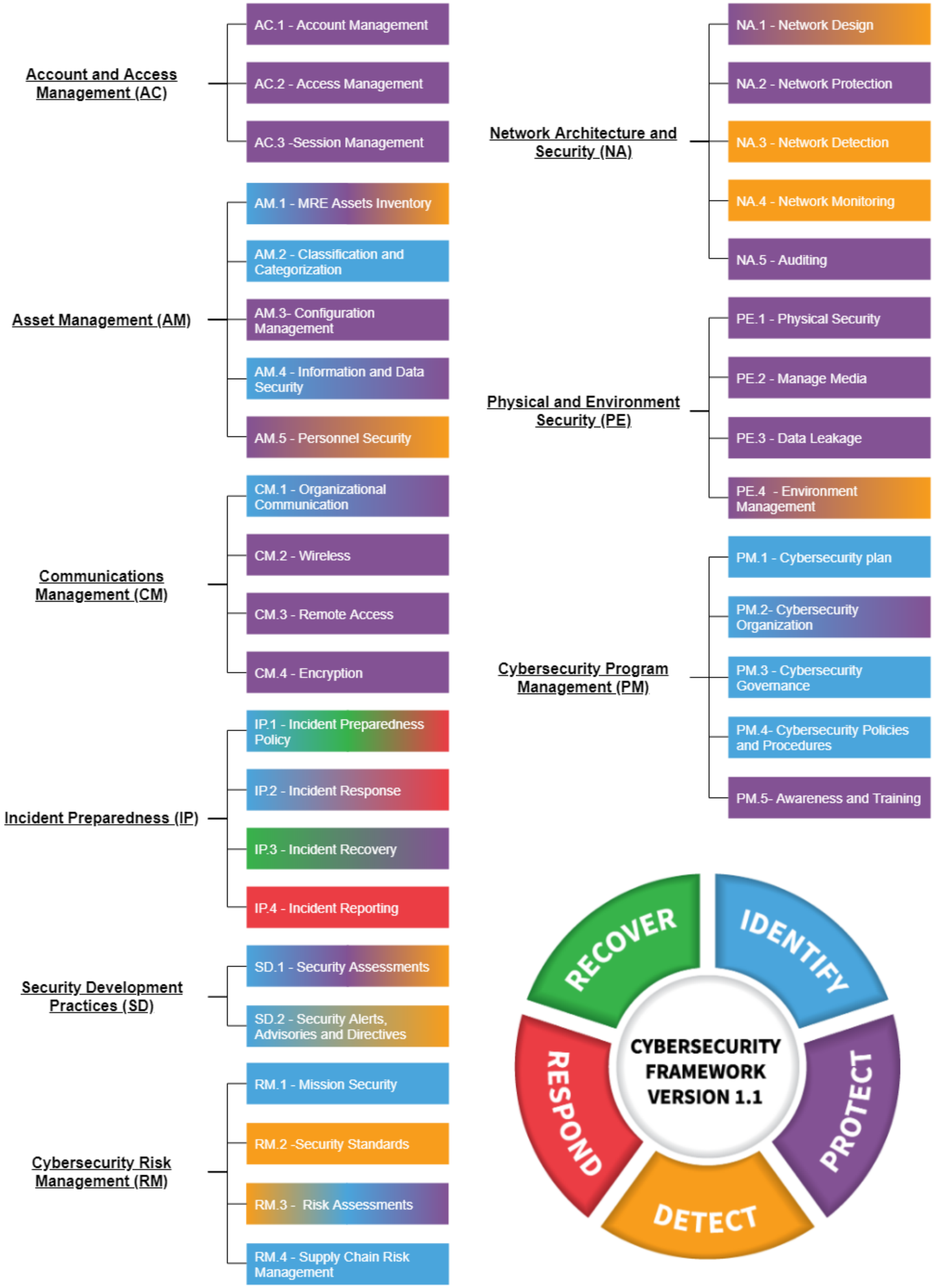

Account and Access Management (AC)
AC.1 - Account Management
AC.2 - Access Management
AC.3 -Session Management
Asset Management (AM)
AM.1 - MRE Assets Inventory
AM.2 - Classification and Categorization
AM.3- Configuration Management
AM.4 - Information and Data Security
AM.5 - Personnel Security
Communications Management (CM)
CM.1 - Organizational Communication
CM.2 - Wireless
CM.3 - Remote Access
CM.4 - Encryption
Incident Preparedness (IP)
IP.1 - Incident Preparedness Policy
IP.2 - Incident Response
IP.3 - Incident Recovery
IP.4 - Incident Reporting
Security Development Practices (SD)
SD.1 - Security Assessments
SD.2 - Security Alerts, Advisories and Directives
Cybersecurity Risk Management (RM)
RM.1 - Mission Security
RM.2 -Security Standards
RM.3 - Risk Assessments
RM.4 - Supply Chain Risk Management
Network Architecture and Security (NA)
NA.1 - Network Design
NA.2 - Network Protection
NA.3 - Network Detection
NA.4 - Network Monitoring
NA.5 - Auditing
Physical and Environment Security (PE)
PE.1 - Physical Security
PE.2 - Manage Media
PE.3 - Data Leakage
PE.4 - Environment Management
Cybersecurity Program Management (PM)
PM.1 - Cybersecurity plan
PM.2- Cybersecurity Organization
PM.3 - Cybersecurity Governance
PM.4- Cybersecurity Policies and Procedures
PM.5- Awareness and Training
RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

Figure 7. MRE System Cybersecurity Best Practices

## 6.0 References

[1] dePeralta F, A Gorton, M Watson, R Bays, J Boles, J Castleberry, B Gorton, and F Powers. 2020. *Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems*. PNNL-29802. Pacific Northwest National Laboratory, Richland, WA.

[2] Sabinno V. 2020. “Energy Sector Cybersecurity Is Vulnerable but Achievable.*” Power Engineering*. Accessed on August 7, 2020 at https://www.power-eng.com/2020/02/12/energy-sector-cybersecurity-is-vulnerable-but-achievable/#gref.

[3] Tucci AE. 2017. “Cyber Risks in the Marine Transportation System.” In R Clark & S Hakim (Eds.), *Cyber-Physical Security. Protecting Critical Infrastructure* (pp. 113-131). Switzerland: Springer.

[4] DOE. 2018. *Multiyear Plan for Energy Sector Cybersecurity*. U.S. Department of Energy. Accessed March 24, 2020 at https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

[5] Neary M, M Previsic, RA Jepsen, MJ Lawson, Y-H Yu, AE Copping, AA Fontaine, KC Hallett, and DK Murray. 2014. *Methodology for Design and Economic Analysis of Marine Energy Conversion (MEC) Technologies*, No. SAND2014-3561C. Sandia National Laboratories, Albuquerque, NM.

[6] LiVecchi A, A Copping, D Jenne, A Gorton, R Preus, G Gill, R Robichaud, R Green, S Geerlofs, S Gore, D Hume, W McShane, C Schmaus, and H Spence. 2019. *Powering the Blue Economy; Exploring Opportunities for Marine Renewable Energy in Maritime Markets*. U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. Washington, D.C. Accessed on March 10, 2020 at https://www.energy.gov/eere/water/powering-blue-economy-exploring-opportunities-marine-renewable-energy-maritime-markets#prizes.

[7] DOE. 2015. *Energy Sector Cybersecurity Framework Implementation Guidance*. Office of Electricity Delivery and Energy Reliability, U.S. Department of Energy. Accessed March 19, 2020 at https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf.

[8] NIST. 2018. *Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)*, Version 1.1, April 2018. National Institute of Standards and Technology https://www.nist.gov/cyberframework.

[9] NIST. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, SP 800-37, Rev. 2. National Institute of Standards and Technology. Accessed March 19, 2020 at https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

[10] Dragos. 2019. *Industrial Control System (ICS) Year in Review: The ICS Landscape and Threat Activity Groups*. Available at https://dragos.com/resource/dragos-2019-ics-year-in-review-the-ics-threat-landscape-and-activity-groups/.

[11] MITRE. 2020 (Updated). “MITRE ATT&CK for ICS Framework.” Accessed March 19, 2020 at https://collaborate.mitre.org/attackics/index.php/Main_Page.

[12] MITRE. 2019 (Updated or Reviewed). “Common Attack Pattern Enumeration and Classification.” Accessed March 19, 2020 at https://capec.mitre.org/.

[13] ESCSWG. 2014. *Cybersecurity Procurement Language for Energy Delivery Systems.* April 2014. Energy Sector Control Systems Working Group. Accessed at http://www.energy.gov/sites/prod/files/2014/04/f15/CybersecProcurementLanguage-EnergyDeliverySystems_040714_fin.pdf.

[14] Dragos. 2020. *Energy Organizations Continue to be Compromised Globally.* Accessed at https://www.dragos.com/blog/industry-news/energy-organizations-continue-to-be-compromised-globally/.

[15] NIST. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4. April 2013. National Institute of Standards and Technology. Gaithersburg, MD.

[16] NIST. 2015. *Guide to Industrial Control Systems (ICS) Security*, SP 800-82, Revision 2. May 2015. National Institute of Standards and Technology. Gaithersburg, MD.

[17] NIST. 2015. *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, SP 800-161, Revision 0. April 2015. National Institute of Standards and Technology. Gaithersburg, MD.

[18] NIST. 2020. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, SP 800-171, Revision 2. February 2020. National Institute of Standards and Technology. Gaithersburg, MD.

[19] OPS. 2013. Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience,* The White House Office of the Press Secretary, dated February 12, 2013.

[20] Federal Power Act, Title 16 U.S. Code (USC) Chapter 12, Subchapter I – Federal Regulation and Development Power. 2018. https://www.govinfo.gov/content/pkg/USCODE-2018-title16/pdf/USCODE-2018-title16-chap12.pdf.

[21] MITRE. 2020 (Updated). “MITRE ATT&CK for Enterprise Matrix.” Accessed August 1, 2020 at https://attack.mitre.org/matrices/enterprise/.

[22] FERC. 2020. *Cybersecurity Incentives Policy White Paper.* Docket AD20-19-000. U.S. Federal Energy Regulatory Commission. Accessed August 1, 2020 at https://www.ferc.gov/sites/default/files/2020-06/notice-cybersecurity.pdf.

[23] U.S. Department of Interior/FERC. 2020. *BOEM / FERC Guidelines on Regulation of Marine Hydrokinetic Energy Projects on the OCS*, Version 3, May 27, 2020. Bureau of Ocean Energy Management/Federal Energy Regulatory Commission. https://www.ferc.gov/sites/default/files/2020-06/Guidance-document-on-Outer-Continental-Shelf-development-with-DOI.pdf.

[24] Marine and Hydrokinetic Renewable Energy Act of 2014. 2014. Senate Report 113-294 [to accompany Senate Bill S. 1419], 113th Congress. https://www.govinfo.gov/content/pkg/CRPT-113srpt294/html/CRPT-113srpt294.htm.

[25] BIMCO. ND. *The Guidelines on Cyber Security Onboard Ships.* Version 3. Accessed on August 11, 2020 at https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

[26] ABS. 2016. *Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations*, Volume 1. September 2016. American Bureau of Shipping, New York, NY. Accessed on August 11, 2020 at https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf.

[27] NIST. 2008. *Guide for Mapping Types of Information and Information Systems to Security Categories,* SP 800-60, Volumes I and II, Revision 1. August 2008. National Institute of Standards and Technology. Gaithersburg, MD

[28] Jang-Jaccard, J and S Nepal. “A Survey of Emerging Threats in Cybersecurity.” *Journal of Computer and System Sciences*. 80:973-993.

[29] O’Neil, R, G Staines, and M Freeman. 2019. *Marine Hydrokinetics Regulatory Processes Literature Review.* PNNL-28608. Pacific Northwest National Laboratory, Richland, WA.

[30] U.S. Department of Interior/BOEM. 2020. *Leasing Outer Continental Shelf*. Department of Interior/ Bureau of Ocean Energy Management. Accessed on August 31, 2020 at https://www.boem.gov/oil-gas-energy/leasing/outer-continental-shelf

# Appendix A – Definitions

Asset
Hardware, software, computer networks, communication methods, applications, and other operational and information technology items that manage data (i.e., collect, use, develope, in transit (received or transmitted), and stored)

Cyberattack
Any attempt to expose, alter, disable, destroy, steal, or gain unauthorized access to or make unauthorized use of an asset

Cybersecurity
Protection of IT/OT assets against the criminal or unauthorized use of electronic data and systems

End User/Market
The intended client or organization that depends on the electricity generated from the marine renewable energy device

Developer
Organizations or manufacturer responsible for the marine renewable energy system design

Information System
Organizational system designed to collect, process, store, and distribute information

Information System Owner
Individual or organization responsible for the maintenance or operation of a marine renewable energy information system

Mitigation Controls
Security configurations or strategies designed to remediate a threat to a system

Operating System
The software that supports a computer’s basic functions, such as scheduling tasks, executing applications, and controlling peripherals

Operating System Owner
Individual or organization responsible for the maintenance or operation of a marine renewable energy operating system

Risk
The product of the likelihood of an event occurring and the consequences (impact) if the event occurs

Threat
Malicious act that intentionally or accidently exploits a vulnerability to damage data, steal data, or disrupt digital life in general (e.g., computer viruses, data breaches, and denial of service attacks)

Threat Event Frequency
Number of times in a year that the threat event occurs

Threat Source
One or more individuals/groups (sources) who are executing a threat

Vulnerability
Weakness or gap in the protection/security of the marine renewable energy system

# Appendix B – MRE Threats and Mitigation Strategies

The MITRE ATT&CK$^{TM}$ (Adversarial Tactics, Techniques and Common Knowledge) Matrix for Enterprise [21] and Industrial Control Systems [10] were reviewed to identify mitigation strategies that should be included in the marine renewable energy (MRE) cybersecurity best practices. Table B.1 identifies the examples of countermeasures and mitigation strategies or the known threats to MRE systems [1].

Table B.1. MRE System Threats and Mitigation Strategies

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| ***Malicious Activity*** | | |
| Brute Force | An attacker attempts to gain access to an MRE asset using trial and error to exhaustively explore all possible secret values to find a value that will unlock an MRE asset. | • Use multifactor authentication. Where possible, also enable multifactor authentication on externally facing services.<br>• Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed.<br>• Establish minimum password requirements.<br>• Proactively reset accounts that are known to be part of breached credentials either immediately or after detecting brute-force attempts. |
| Elevation of Privileges | An adversary exploits an MRE weakness, enabling the adversary to elevate his/her permissions and perform an action that the adversary is not authorized to perform. | • Update software regularly and employ patch management for endpoints and servers.<br>• Complete privilege account management by removing users from the local administrator group on systems. By requiring a password, even if an adversary can get terminal access, the adversary must know the password to run anything in the "sudoers" file. Setting the timestamp timeout to 0 will require the user to input his/her password every time "sudo" is executed. |
| Denial of Service | An attacker attempts to prevent normal MRE staff and/or customer activity. | • Depending on flood volume, on-premises filtering may be possible by blocking source addresses sourcing the attack, blocking ports that are being targeted, or blocking protocols being used for transport. |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| Data Theft or Identity Theft | An adversary steals MRE development/operational data. or personal identification information | • Consider implementing information technology (IT) disaster recovery plans that contain procedures for making regular data backups that can be used to restore data. |
| Malware | An adversary installs or adds malicious logic (also known as malware) into a seemingly benign MRE component of a fielded system. | • Update software regularly and employ patch management for endpoints and servers.<br>• Implement antivirus capabilities and establish firewall rules.<br>• Disable Autorun if it is unnecessary. Disallow or restrict removable media at an organizational policy level if it is not required for business operations. |
| Ransomware | An adversary installs and executes malicious code on the MRE system to try to achieve a negative technical impact and then to demand payment for removing the code. | • Update software regularly and employ patch management for endpoints and servers.<br>• Verify that data backup procedures exist and IT disaster recovery plans that contain procedures for making regular data backups that can be used to restore data.<br>• Provide user training on cyber best practices. |
| Social Engineering (Phishing) | An attacker masquerades as a legitimate entity with which the MRE staff might do business in order to prompt the user to reveal some confidential information (very frequently authentication credentials). | • Antivirus can automatically quarantine suspicious files.<br>• Use network intrusion prevention systems and systems designed to scan and remove malicious content or links and to block activity.<br>• Determine if certain websites or attachment types (e.g., .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk. |
| Supply Chain | An attacker disrupts the MRE supply chain life cycle by manipulating system hardware, software, or services. | • Implement a Supply Chain Risk Management Program.<br>• A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files, and documentation. |
| Remote Services | An adversary uses stolen credentials to leverage remote services such as virtual private network, Remote Desktop Protocol, telnet, Secure Shell, and virtual network computing to log into the MRE system. | • Use multifactor authentication for remote service login.<br>• Minimize permissions and access for service accounts to limit impact of exploitation. |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| | | • Segment networks and systems appropriately to reduce access to critical systems and services to controlled methods.<br>• Update software regularly by employing patch management for endpoints and servers. |
| Targeted Malware | An adversary develops MRE-targeted malware that takes advantage of a known vulnerability in an MRE system. | • Implement antivirus with automatic quarantine capabilities.<br>• Use network intrusion prevention systems and systems designed to scan and remove malicious content. |
| ***Sniffing, Tampering, Hijacking*** | | |
| Eavesdropping of Sensitive Data | An adversary intercepts a form of communication (e.g., text, audio, video) via software (e.g., microphone and audio recording application), hardware (e.g., recording equipment), or physical means (e.g., physical proximity) to gain unauthorized access to sensitive information. | • Special care should be taken to make sure passwords used with encrypted and non-encrypted protocols are not the same.<br>• Password authentication can be used as a barrier, in addition to restricting user account file access according to the principle of least privilege. The default for newly created accounts should be minimal to reduce adversary movement capabilities.<br>• Encrypt important information to reduce an adversary’s ability to use data. |
| Sniffing Communication Traffic | An adversary intercepts information transmitted between two MRE components. Threat is similar to man-in-the-middle attacks but is entirely passive. | • Prior to wireless network installation, survey the area to determine the antenna location and strength that minimizes exposure of the network. An adversary can extend the effective range of a wireless local area network with powerful directional antennas.<br>• Isolate wireless access points and data servers for wireless worker devices on their own network with documented and minimal (single if possible) connections to the industrial control system (ICS) network.<br>• Segmenting the network with virtual local area networks allows switches to enforce security policies and segregate traffic at the Ethernet layer. Proper segmentation helps mitigate the risk of broadcast storms resulting from port scans. Assigning each automation cell to a single virtual local area network limits unnecessary traffic flooding.<br>• Implement virtual private networks to further restrict access in and out of control system computers and |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
|  |  | controllers, which help remove unauthorized, non-essential traffic from the intermediary network.<br>• In ICS environments with dial-up modems, disconnect the modems when not in use or automate their disconnection after being active for a given amount of time, if reasonable.<br>• Network services will often transmit in plain text, making third-party eavesdropping easy. When communications over both encrypted and non-encrypted protocols with passwords exist, be sure to use different passwords.<br>• Implementing challenge/response authentication eliminates the risk of discovery or replay that traditional password exchange has.<br>• Secure and restrict authorization to the control room and the physical environment. Make sure ICS and IT network cables are kept separate and that devices are locked up when possible.<br>• Encrypt and protect the integrity of wireless device communications, while taking care not to degrade end device performance. Open Systems Interconnection Layer 2 encryption, rather than Layer 3, can reduce encryption-based latency. Hardware accelerator solutions for cryptographic functions may also be considered.[5]<br>• Verify that all wireless traffic is encrypted appropriately. Use Kerberos, SSL, and multifactor authentication wherever possible. Monitor switches and network for span port usage, ARP/DNS poisoning, and router reconfiguration.[5]<br>• Make use of antivirus and malware detection tools to further secure the environment. Monitor the network and enforce access control practices, such as whitelisting, to reduce points of contact to and from control system devices, where applicable. Implement heuristics to detect monitoring and invasive probing activity on the network.<br>• Identify and block potentially malicious software that may be used to sniff or analyze network traffic by using whitelisting[6] tools, like AppLocker,[7][8] or Software Restriction Policies[9] where appropriate.[10] |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| Network Reconnaissance | An adversary engages in probing and exploration activities to identify MRE network constituents and properties to learn as much as possible about the composition, configuration, and security mechanisms of the MRE system or network. | • Update software regularly and employ patch management for endpoints and servers.<br>• Special care should be taken to make sure passwords used with encrypted and non-encrypted protocols are not the same.<br>• Use antivirus and malware detection tools to further secure the environment. Monitor the network and enforce access control practices, such as whitelisting, to reduce points of contact to and from control system devices, where applicable. Implement heuristics to detect monitoring and invasive probing activity on the network. |
| Vulnerability Scanning | An attacker engages in scanning activity to find vulnerable MRE software versions or types, such as operating system versions or network services. | • Update software regularly and employ patch management for endpoints and servers.<br>• Segment networks and systems appropriately to reduce access to critical systems and services to controlled methods. |
| Man-in-the-Middle | An adversary places him/herself in between two MRE components to attack the communication, resulting in all data first going to the attacker before being passed on to the other component as if it were never observed. | • Encrypt and protect the integrity of wireless device communications, while taking care not to degrade end device performance. Open Systems Interconnection Layer 2 encryption, rather than Layer 3, can reduce encryption-based latency. Hardware accelerator solutions for cryptographic functions may also be considered.[4]<br>• Special care should be taken to make sure passwords used with encrypted and non-encrypted protocols are not the same. Password lockout policies can be enforced, but take care to balance this with operational needs that might result in a few failed login attempts in stressful situations.[4]<br>• Implementing challenge/response authentication eliminates the risk of discovery or replay that traditional password exchange has.[4]<br>• Restrict access to control rooms, portable devices, and removable media, which should be locked down and physically secured.[4]<br>• Unauthorized and suspicious media should be avoided and kept away from systems and the network.[4]<br>• Make sure ICS and IT network cables are kept separate and that devices are locked up when possible.[4] |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| | | • Virtual private networks can be used to provide secure access from an untrusted network to the ICS control network and restrict access to and from host computers.[4]<br>• Depending on how it is deployed, an intrusion detection system might be able to detect or help with the detection of a man-in-the-middle attack. |
| ***Accidental Damage*** | | |
| Incorrect Operational Technology System Administration | Erroneous actions taken by MRE operators/engineers, IT, and/or vendors when executing their everyday responsibilities. | • Manage accounts and access using least privilege.<br>• Implement contingency plans to detect erroneous actions and implement continuous backup of data. |
| Misconfigured IT-Managed Security Services | Dependent IT security managed services not configured correctly to monitor MRE system. | • Update software regularly and employ patch management for endpoints and servers.<br>• Block unused ports and protocols that would otherwise be able to be used in an attack. |
| Data Loss | The exposure of MRE proprietary or business-sensitive information through either data theft or data leakage. | • Restrict access to control rooms, portable devices, and removable media, which should be locked down and physically secured. Unauthorized and suspicious media should be avoided and kept away from systems and the network. Keep track of cables to make sure the ICS and IT environments remain separate and no interceptive, adversarial devices are installed.<br>• Encrypt important information to reduce an adversary's ability to use data.<br>• Limit the use of USB storage devices and removable media within a network.<br>• Identify critical business and system processes that may be targeted by adversaries and work to isolate and secure those systems against unauthorized access and tampering.<br>• Consider implementing IT disaster recovery plans that contain procedures for making regular data backups that can be used to restore data. |
| ***Physical Attacks*** | | |
| Sabotage | An adversary deliberately manipulates the MRE safety system operation such that it either 1) does not operate when needed or 2) | • Restrict physical access to MRE system assets and secure assets in locations not accessible by unauthorized users. |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| | performs incorrect control actions that damage the MRE system. | |
| Vandalism | An adversary causes physical damage to an MRE asset or other resource. | • Restrict physical access to MRE system assets and secure assets in locations not accessible by unauthorized users. |
| Theft | An adversary steals a physical MRE system asset or other resource. | • Restrict physical access to MRE system assets and secure assets in locations not accessible by unauthorized users.<br>• Implement barriers, locks, anchors, or other mechanisms to deter theft of an asset.<br>• Use a physical protection system that alarms if unauthorized access is detected. |
| Unauthorized Access | An adversary gains physical access to an MRE asset or other resource without permission. | • Restrict physical access to MRE system assets and secure assets in locations not accessible by unauthorized users.<br>• Implement barriers, locks, anchors, or other mechanisms to deter theft of an asset.<br>• Use a physical protection system that alarms if unauthorized access is detected. |
| Terrorism | An adversary uses traditional attack methods (e.g., bomb) to destroy, incapacitate, or exploit the MRE system for religious, political, or ideological reasons. | • Restrict physical access to MRE system assets and secure assets in locations not accessible by unauthorized users.<br>• Consider implementing IT disaster recovery plans that contain procedures for making regular data backups that can be used to restore data. |
| Hacktivism | An adversary uses technology to destroy, incapacitate, or exploit the MRE system to promote a political or social agenda. | • Verify that cybersecurity policies and procedures exist and systems are being maintained. |
| Organized Crime | An adversary (e.g., pirates) attacks the MRE system for monetary gain. | • Restrict physical access to MRE system assets and secure assets in locations not accessible by unauthorized users.<br>• Disable Autorun if it is unnecessary, especially if the MRE system is in remote locations. Disallow or restrict removable media at an organizational policy level if it is not required for business operations. |
| ***Infrastructural/Component Failures and Malfunctions*** | | |

| MRE Threat Types and Subcategories | Description | Examples of Counter Measures and Mitigation Strategies |
|---|---|---|
| Failures or Malfunctions of MRE System or Devices | A failure or malfunction of the MRE system or resource. | • Implement contingency plan when operation of systems is affected (e.g., fail safe position). |
| Known Vulnerabilities | An MRE system asset with known vulnerabilities that could be exploited by an adversary. | • Develop vulnerability management plan and periodically scan systems for known vulnerabilities<br>• Keep abreast of cybersecurity alerts from industry sources, such as Industrial Control Systems-Cyber Emergency Response Team. |
| Improper Network Architecture | An adversary engages undetected in lateral movement through the network (e.g., nodes, hosts, devices, and routes). | • Segment networks and systems appropriately to reduce access to critical systems and services to controlled methods. |
| Disruption of Service Providers | An unplanned event that causes the MRE system to be inoperable for a length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). | • Implement contingency plan when operational environment is affected (e.g., loss of power). |
| ***Disasters*** | | |
| Environmental | A catastrophic human incident causing unfavorable environmental conditions, such as a shipwreck. | • Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore data. |
| Natural | A major adverse event resulting from natural processes of the Earth, such as a cyclonic storm, tsunami, heavy winds. | • Consider implementing IT disaster recovery plans that contain procedures for taking regular data backups that can be used to restore data. |

# Appendix C – Cybersecurity Risk Categorization Worksheet

Marine renewable energy (MRE) owners and operators can use this risk assessment form to determine the risk posture of an MRE system when deployed. The MRE stakeholder will rate the MRE system and end-use configuration by determining whether its cybersecurity vulnerability (low, moderate or high) and the consequences a cybersecurity incident would have on the mission of its end user (low, moderate or high). The MRE system and its configuration can then be ranked as risk level 1, 2, or 3. The cybersecurity guidance in the Focus 2 report describes the security controls for each risk level.

| | | | |
|---|---|---|---|
| **MRE System** | System type (e.g. wave absorber, oscillating flap, surge flap, water column, etc.) | | |
| **End Use** | Mission Purpose Statement (e.g. application of system end use) | | |
| **Threat Metrics** | **MRE System Vulnerability Categorization** | | |
| | **LOW** | **MODERATE** | **HIGH** |
| 1. Information Technology/Operational Technology (IT/OT) Assets and Network Architecture | No IT/OT systems. | Communication to IT/OT assets is provided by local networks. | Communication to IT/OT assets can be performed remotely (i.e., wireless, Bluetooth, radiofrequency, satellite). |
| 2. Geography | MRE system is continuously monitored electronically or physically (i.e. detection capability provided on an MRE system such as satellite observation/GPS, cameras, sensors, etc.). | MRE system is intermittently monitored electronically or physically (i.e. non-continuous monitoring, physically patrolled at least once a week, no alert notification of physical security breach, etc.). | MRE system is not monitored electronically or physically (i.e. not physically patrolled greater than once a week). |
| 3. Physical Accessibility | Assets are enclosed in physically locked containers and access is managed and monitored. | Assets are enclosed in physically locked containers and access is not managed and monitored. | Assets are enclosed in containers that are accessible by anyone (i.e., unlocked, unmanaged access, etc.) or assets that are not physically protected. |
| 4. Connectivity with External Networks | Not connected to external networks or connection to external networks not more than once a month. | Connection to external networks at least weekly. | Connected to external networks continuously or daily. |

| | | | |
|---|---|---|---|
| **MRE System** | System type (e.g. wave absorber, oscillating flap, surge flap, water column, etc.) | | |
| **End Use** | Mission Purpose Statement (e.g. application of system end use) | | |
| **Threat Metrics** | **MRE System Vulnerability Categorization** | | |
| | **LOW** | **MODERATE** | **HIGH** |
| 5. Access/User Controls | Identification and authentication of users are managed (e.g., least privilege established, role-based, multifactor authentication). | Identification and authentication of users are partially managed (e.g., multi-users on same account allowed, least privilege not established). | Identification and authentication of users is not managed. |
| 6. Roles and Responsibilities | Organization has dedicated staff to manage cybersecurity (e.g., Chief Information Security Officer, incident response roles). | Organization has partially dedicated staff to manage cybersecurity (e.g., staff member shares other roles outside of cybersecurity). | Organization does not have any dedicated staff to manage cybersecurity. |
| 7. Security Controls on Software, Hardware, and Firmware | Preventive measures (e.g., patch management, encryption, antivirus or continuous security monitoring, automatic updates, etc.) and detective security controls (e.g., host or network intrusion detection). | Security controls that prevent or detect network communications are implemented. | Minimal security control to network (e.g., firewall, password protection). |
| VULNERABILITY (LIKELIHOOD) SCORE | | | |

| | | | |
|---|---|---|---|
| **MRE System** | System type (e.g. wave absorber, oscillating flap, surge flap, water column, etc.) | | |
| **End Use** | Mission Purpose Statement (e.g. application of system end use) | | |
| **Consequence Factors** | **MRE System Consequences** | | |
| | **LOW**<br>**Score = 1** | **MODERATE**<br>**Score = 2** | **HIGH**<br>**Score = 3** |
| 1. Impact on End User's Mission. | Organization can perform its primary functions, but the effectiveness of the functions is not noticeably reduced. | Organization can perform its primary functions, but the effectiveness of the functions is significantly reduced. | Organization cannot perform one or more of its primary functions. |
| 2. Physical Impact to MRE System (e.g., Loss of Control, Disruption of Operation). | No physical damage to ICS and supporting infrastructure or minor damage (i.e., redundant controls available, non-digital | Significant physical damage to assets, supporting infrastructure, and human safety (e.g., | Major physical damage to assets and supporting infrastructure and impact to environment (e.g., damage to |

| | | | |
|---|---|---|---|
| **MRE System** | System type (e.g. wave absorber, oscillating flap, surge flap, water column, etc.) | | |
| **End Use** | Mission Purpose Statement (e.g. application of system end use) | | |
| **Consequence Factors** | **MRE System Consequences** | | |
| | **LOW**<br>**Score = 1** | **MODERATE**<br>**Score = 2** | **HIGH**<br>**Score = 3** |
| | mechanisms provided such as audio alarms, manual valves to protect the physical boundary). | manipulation of controls). | electric generation and delivery). |
| 3. Loss of Data or Information (e.g., Impact of Loss of Confidentiality, Integrity, and Availability) | No impact to mission or end use. | Minor impact to mission or end use. | Major impact to mission or end use. |
| 4. Impact on Interconnected Networks (e.g., Enterprise Systems, End User's Systems, Other ICS Networks) | No impact or no connectivity to other networks. | Moderate impact due to ability to isolate connectivity with other networks. | Major impact due to inability to isolate connectivity with other networks. |
| 5. Financial Impact (e.g., Loss of Productivity and Income, Response Cost, Recovery Cost, Fines and Judgments.) | None or minor financial loss as defined by organization. | Significant financial loss as defined by organization. | Major financial loss as defined by organization. |
| CONSEQUENCE (IMPACT) SCORE | | | |
| MRE SYSTEM RISK LEVEL [Note1] | | | |

Note 1: Use the MRE System Cybersecurity Risk Ranking Chart (Table C.1) to determine the risk level for the assets and configuration. Use the Cybersecurity Guidance document to determine the baseline security controls to implement commensurate with the risk level.

Table C.1. MRE System Cybersecurity Risk Ranking Chart

| **Vulnerability** | **Consequences of Cyberattack** | | |
|---|---|---|---|
| | **LOW** | **MODERATE** | **HIGH** |
| **LOW** | 1 | 2 | 3 |
| **MODERATE** | 1 | 2 | 3 |
| **HIGH** | 2 | 3 | 3 |

# Appendix D – Summary of Marine Renewable Energy Cybersecurity Best Practice Guidance

This appendix summarizes the cybersecurity best practices developed from the related industry resources (e.g., NIST CSF [8], NERC CIP Standards, NIST SP 800-53 [15], ESCSWG [13], and BIMCO [25]). Table D.1 is an overview of the MRE cybersecurity categories, 36 best practices, and 86 security measures developed for marine renewable energy (MRE) systems in section 4.2 of this report. The 86 security measures are further described by Risk Levels 1, 2, or 3 in Table D.1 based on the description Section 4.1 of this report and Appendix C worksheet.

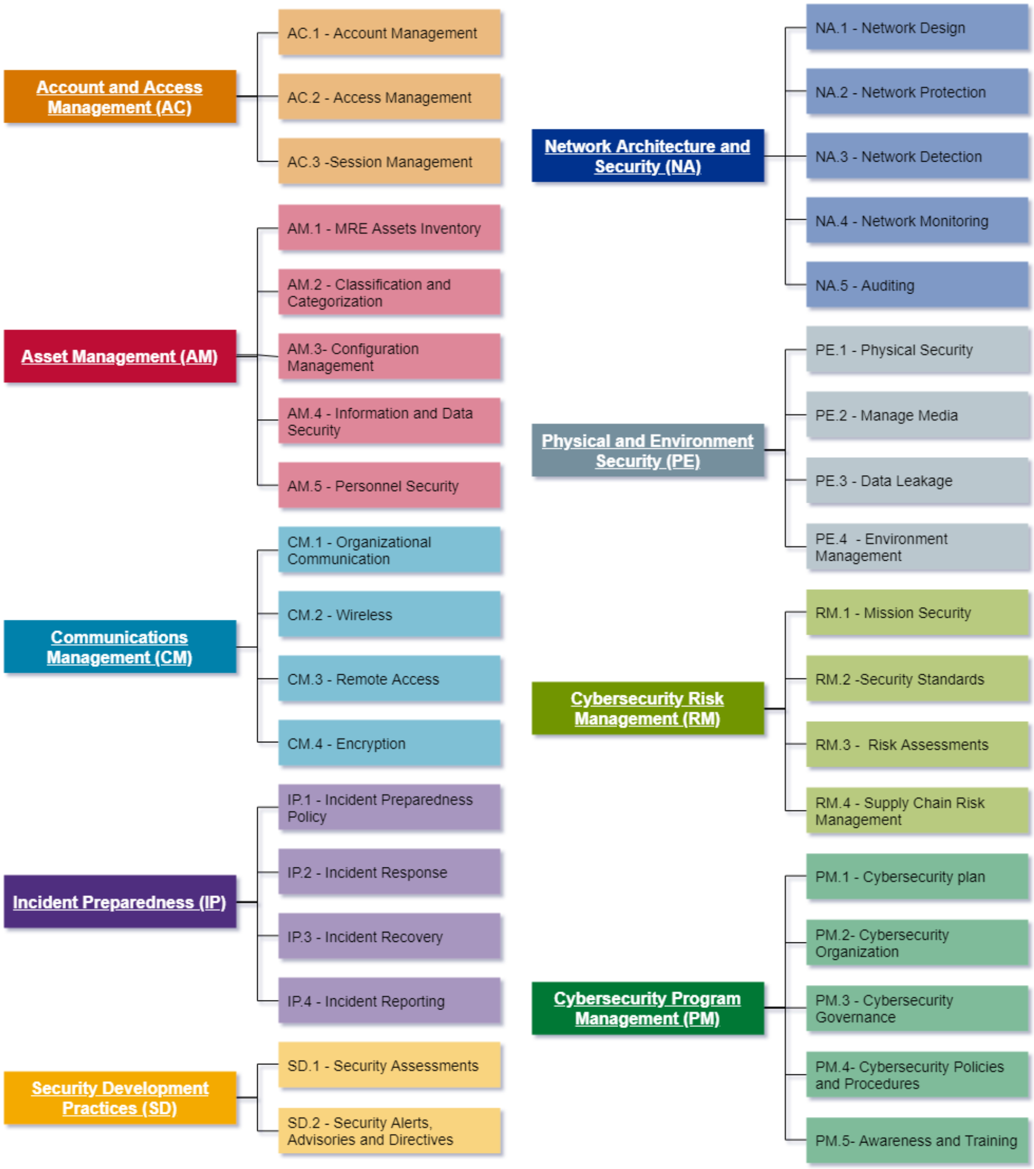

Account and Access Management (AC)
AC.1 - Account Management
AC.2 - Access Management
AC.3 -Session Management
Asset Management (AM)
AM.1 - MRE Assets Inventory
AM.2 - Classification and Categorization
AM.3- Configuration Management
AM.4 - Information and Data Security
AM.5 - Personnel Security
Communications Management (CM)
CM.1 - Organizational Communication
CM.2 - Wireless
CM.3 - Remote Access
CM.4 - Encryption
Incident Preparedness (IP)
IP.1 - Incident Preparedness Policy
IP.2 - Incident Response
IP.3 - Incident Recovery
IP.4 - Incident Reporting
Security Development Practices (SD)
SD.1 - Security Assessments
SD.2 - Security Alerts, Advisories and Directives
Network Architecture and Security (NA)
NA.1 - Network Design
NA.2 - Network Protection
NA.3 - Network Detection
NA.4 - Network Monitoring
NA.5 - Auditing
Physical and Environment Security (PE)
PE.1 - Physical Security
PE.2 - Manage Media
PE.3 - Data Leakage
PE.4 - Environment Management
Cybersecurity Risk Management (RM)
RM.1 - Mission Security
RM.2 -Security Standards
RM.3 - Risk Assessments
RM.4 - Supply Chain Risk Management
Cybersecurity Program Management (PM)
PM.1 - Cybersecurity plan
PM.2- Cybersecurity Organization
PM.3 - Cybersecurity Governance
PM.4- Cybersecurity Policies and Procedures
PM.5- Awareness and Training

Figure D.1 – Overview of MRE Cybersecurity Requirements by Category

**Color Key**

| AC | AM | CM | IP | NA | PE | PM | RM | SD |
|---|---|---|---|---|---|---|---|---|

Table D.1. Risk-based Cybersecurity Best Practices for MRE Systems

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| **Account and Access (AC) Management** | | | | | |
| **AC.1 – Account Management** | AC.1(1) – Manage Accounts | **CSF:** PR.AC-1, PR.AC-4<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** AC-1, AC-2, AC-6, AC-8, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11<br>**ESCSWG:** 2.3 | X | X | X |
| | AC.1(2) – Configuration of Accounts | **CSF:** PR.AC-4<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** AC-6<br>**ESCSWG:** 2.3 | X | X | X |
| **AC.2 – Access Management** | AC.2(1) – Least Privilege and Separation of Duties | **CSF:** PR.AC-4. PR.AC-6<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-007-6<br>**NIST SP 800-53R4:** AC-1, AC-2, AC-3, AC-5, AC-6, AC-10, AC-11, AC-12, AC-14, AC-16, AC-19, AC-24, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, PE-2, PS-3<br>**ESCSWG:** 2.2 | X | X | X |
| | AC.2(2) – Authentication | **CSF:** PR.AC-7<br>**NERC CIP:** None<br>**NIST SP 800-53R4**: AC-7, AC-8, AC-9, AC-11, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **ESCSWG:** 2.5, 5.1, 7.1 | | | |
| | AC.2(3) – Access Protocols | **CSF:** PR.AC-1, PR.AC-6<br>**NERC CIP:** CIP-005-5<br>**NIST SP 800-53R4:** AC-2**,** AC-3, IA-2<br>**ESCSWG:** 2.4 | X | X | X |
| **AC.3 – Session Management** | AC.3(1) – Restrict Multiple Concurrent Logins | **CSF:** PR.AC-5<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-007-6<br>**NIST SP 800-53R4:** AC-10<br>**ESCSWG:** 2.4 | | | X |
| | AC.3(2) – Session Termination | **CSF:** PR.AC-4<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-007-6<br>**NIST SP 800-53R4:** AC-11, AC-12<br>**ESCSWG:** 2.4 | | | X |
| | AC.3(3) – Encryption, Digital Signing | **CSF:** PR.AC-4<br>**NERC CIP:** CIP-010-3<br>**NIST SP 800-53R4:** AC-2, PE-2<br>**ESCSWG:** 2.4 | | X | X |
| **Asset Management (AM)** | | | | | |
| **AM.1 – MRE Assets Inventory** | AM.1(1) – Asset Inventory | **CSF**: ID.AM-1, ID.AM-2, ID.AM-4, ID.AM-5<br>**NERC CIP:** CIP-002-5.1, CIP-003-8, CIP-005-5, CIP-009-6<br>**NIST SP 800-53R4:** AC-20, CP-2, CM-8, SA-9, PM-5<br>**ESCSWG:** 3.6 | X | X | X |
| | AM.1(2) – Manage Assets | **CSF**: PR.DS-3<br>**NERC CIP:** CIP-002-5.1, CIP-003-8, CIP-005-5, CIP-009-6<br>**NIST SP 800-53R4:** CM-8, MP-6, PE-16<br>**ESCSWG:** 3.6 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | AM.1(3) – Maintenance of Assets | **CSF:** PR.MA-1. PR.MA-2, DE.DP-3<br>**NERC CIP:** CIP-002-5.1, CIP-003-8, CIP-005-5, CIP-009-6<br>**NIST SP 800-53R4:** MA-2, MA-3, MA-4, MA-5, MA-6<br>**ESCSWG:** 3.6 | X | X | X |
| **AM.2 – Classification and Categorization** | AM.2(1) – Classify and Categorize MRE Assets | **CSF:** ID.AM-5<br>**NERC CIP:** CIP-002-5.1, CIP-003-8, CIP-005-5, CIP-009-6<br>**NIST SP 800-53R4:** RA-2<br>**ESCSWG:** None | X | X | X |
| **AM.3 – Configuration Management** | AM.3(1) – Configuration Baseline | **CSF:** PR.IP-1<br>**NERC CIP:** CIP-003-8, CIP-010-2, CIP-003-8<br>**NIST SP 800-53R4:** CM-2, CM-3, CM-4, CM-5, C-6, CM-7, CM-9, SA-10<br>**ESCSWG:** None | X | X | X |
| | AM.3(2) – Configuration Management Process | **CSF:** PR.IP-3<br>**NERC CIP:** CIP-010-2, CIP-003-8<br>**NIST SP 800-53R4:** CM-1, CM-2, CM-3, CM-4, CM-5, C-6, CM-7, CM-9, SA-10<br>**ESCSWG:** 2.1, 2.2, 2.7, 2.8, 3.5, 4.1, 4.2, 6.1 | X | X | X |
| | AM.3(3) – Life Cycle Security | **CSF:** PR.IP-2<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** SA-3, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-16, SI-17<br>**ESCSWG:** 3.1 | X | X | X |
| | AM.3(4) – Manage Data Environment | **CSF:** PR.DS-7<br>**NERC CIP:** CIP-003-8, CIP-005-5, CIP-010-2<br>**NIST SP 800-53R4:** CM-2<br>**ESCSWG:** 2.7, 6.1 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | AM.3(5) – Integrity Checks | **CSF:** PR.DS-8<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** SA-10, SI-7<br>**ESCSWG:** 2.2, 2.8, 3.4, 3.6 | | X | X |
| | AM.3(6) – Backup of Information | **CSF:** PR.IP-4<br>**NERC CIP:** CIP-009-6<br>**NIST SP 800-53R4:** CP-4, CP-6, CP-9<br>**ESCSWG:** None | | X | X |
| **AM.4 – Information and Data Security** | AM.4(1) – Data Flow | **CSF:** ID.AM-5<br>**NERC CIP:** CIP-002-5, CIP-003-8, CIP-005-5, CIP-009-6<br>**NIST SP 800-53R4:** CP-2, RA-2, SA-14, SC-6<br>**ESCSWG:** 2.7, 3.6, 6.6, 7.1 | X | X | X |
| | AM.4(2) – Protect CIA of Data | **CSF:** PR.DS-1, PR.DS-2, PR.DS-4, PR.DS-5<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-007-6, CIP-011-2, CIP-005-5, CIP-009-6<br>**NIST SP 800-53R4:** CA-7, MP-8, PL-8, SC-8, SC-12, SC-28<br>**ESCSWG:** 2.7, 3.6, 6.6, 7.1 | X | X | X |
| | AM.4(3) – Maintenance of Data Protection and Destruction Processes | **CSF:** PR.IP-7, PR.IP-8<br>**NERC CIP:** CIP-011-2, CIP-010-2, CIP-008-5<br>**NIST SP 800-53R4:** MP-6, CA-7, CP-2, SI-4<br>**ESCSWG:** | X | X | X |
| | AM.4(4) – Destruction of Data | **CSF:** PR.IP-6<br>**NERC CIP:** CIP-011-2, CIP-010-2, CIP-008-5<br>**NIST SP 800-53R4:** MP-6<br>**ESCSWG:** 2.10 | X | X | X |
| | AM.4(5) – Protection of CUI | **CSF:** ID.AM-3, PR.DS-1, PR.DS-2, PR-DS-3, PR.DS-4, PR.PT-2, DE.AE-1<br>**NERC CIP:** CIP-011-2<br>**NIST SP 800-53R4:** AC-4, CA-3, MP-5 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **ESCSWG:** 2.7, 2.10, 3.6, 6.6, 7.1 | | | |
| **AM.5 – Personnel Security** | AM.5(1) – Personnel Protection | **CSF:** PR.IP-11<br>**NERC CIP:** CIP-004-6<br>**NIST SP 800-53R4:** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7. PS-8<br>**ESCSWG:** 2.2**,** 3.5, 5.2 | X | X | X |
| | AM.5(2) – Monitor Personnel Activity | **CSF:** DE.CM-3, DE.CM-7<br>**NERC CIP**: CIP-003-8, CIP-004-6, CIP-006-6, CIP-007-6<br>**NIST SP 800-53R4:** AC-2, AU-12, CA-7, CM-3, CM-7, CM-8, CM-10, CM-11, PE-3, PE-6, SI-4<br>**ESCSWG:** 2.2, 2.6, 2.7, 2.8**,** 3.5, 4.1 | X | X | X |
| **Communications Management (CM)** | | | | | |
| **CM.1 – Organizational Communication** | CM.1(1) -Communication Mapping | **CSF:** ID.AM-3<br>**NERC CIP:** CIP-002-5, CIP-003-8, CIP-005-5, CIP-011-2, CIP-012-1<br>**NIST SP 800-53R4:** AC-4, CA-3, CA-9, PL-8<br>**ESCSWG:** 2.7 | | X | X |
| | CM.1(2) -Communication Restrictions | **CSF:** PR.PT-4<br>**NERC CIP:** CIP-002-5, CIP-003-8, CIP-005-5, CIP-011-2, CIP-012-1<br>**NIST SP 800-53R4:** AC-4, SC-3, SC-7, SC8, SC-39<br>**ESCSWG:** 2.7.4, 2.7.5 | X | X | X |
| **CM.2 – Wireless** | CM.2(1) – Wireless Communication Protocols | **CSF:** PR.PT-4<br>**NERC CIP:** CIP-002-5, CIP-003-8, CIP-004-6, CIP-005-5, CIP-010-2, CIP-011-2<br>**NIST SP 800-53R4:** AC-18, AC-19<br>**ESCSWG:** 5.3, 6.1 | | X | X |
| | CM.2(2) – Use Restrictions | **CSF:** PR.PT-4<br>**NERC CIP:** CIP-005-5, CIP-010-2, CIP-011-2<br>**NIST SP 800-53R4:** AC-18, SC-5, SC-40 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **ESCSWG:** 6.1 | | | |
| | CM.2(3) – Network Rules Between Wireless and Wired | **CSF:** PR.IP-1<br>**NERC CIP:** CIP-004-5, CIP-005-5, CIP-010-2<br>**NIST SP 800-53R4:** CM-6, PE-18, SC-40<br>**ESCSWG:** 6.1 | | X | X |
| **CM.3 – Remote Access** | CM.3(1) – Managed Devices | **CSF:** PR.AC-3<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-005-5, CIP-007-6<br>**NIST SP 800-53R4:** AC-1, AC-17, AC-19, AC-20, SC-15<br>**ESCSWG:** 2.7 | X | X | X |
| | CM.3(2) – Virtual Private Network, Bastion Host | **CSF:** PR.DS-2, PR.DS-5<br>**NERC CIP:** CIP-003-8, CIP-005-5<br>**NIST SP 800-53R4:** SC-8<br>**ESCSWG:** 2.7 | | X | X |
| | CM.3(3) – Usage Restrictions | **CSF:** PR.AC-3, PR.PT-4<br>**NERC CIP:** CIP-004-6, CIP-005-5<br>**NIST SP 800-53R4:** AC-17, AC-20, SC-15<br>**ESCSWG:** 2.5, 2.7, 5.2 | X | X | X |
| **CM.4 – Encryption** | CM.4(1) – Cryptographic System Documentation | **CSF:** PR.DS-5<br>**NERC CIP:** CIP-003-8, CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** SC-13<br>**ESCSWG:** 7.1, 7.2 | | X | X |
| | CM.4(2) – Manage Cryptographic Key | **CSF:** PR.DS-1, PR.DS-2<br>**NERC CIP:** CIP-003-8, CIP-005-5, CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** SC-12<br>**ESCSWG:** 7.1, 7.2 | | X | X |
| **Incident Preparedness (IP)** | | | | | |
| | IP.1(1) – Incident Preparedness Policy | **CSF:** RS.RP-1, RS.AN-5, RC.RP-1<br>**NERC CIP:** CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| **IP.1 – Incident Preparedness Policy** | | **NIST SP 800-53R4:** CP-1, CP-2, IR-1, IR-4, IR-8<br>**ESCSWG:** None | | | |
| | IP.1(2) – Incident Preparedness with Suppliers and Third-Party Partners | **CSF:** ID.SC-5<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9<br>**ESCSWG:** None | | X | X |
| **IP.2 - Incident Response** | IP.2(1) – Incident Response Plan | **CSF:** RS.RP-1<br>**NERC CIP:** CIP-008-6<br>**NIST SP 800-53R4:** CP-1, CP2, IR-1, IR-4, IR-5, IR-7, IR-8, IR-9, SI-17<br>**ESCSWG:** None<br>**Other:** NIST SP 800-61 | X | X | X |
| | IP.2(2) – Incident Response Team Training | **CSF:** PR.AT-1<br>**NERC CIP:** CIP-004-6, CIP-008-6<br>**NIST SP 800-53R4:** IR-2, IR-3<br>**ESCSWG:** None | | X | X |
| | IP.2(3) – Periodic Review and Update of IPP | **CSF:** RS.IM-1, RS.IM-2<br>**NERC CIP:** CIP-003-8, CIP-005-5, CIP-006-6, CIP-007-6, CIP-008-5<br>**NIST SP 800-53R4:** IR-1, IR-8<br>**ESCSWG:** None | X | X | X |
| | IP.2(4) – Incident Analysis | **CSF:** RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.AN-5, RS-MI-3<br>**NERC CIP:** CIP-003-8, CIP-006-6, CIP-007-6, CIP-008-5, CIP-010-2<br>**NIST SP 800-53R4:** CP-2, IR-4, IR-8<br>**ESCSWG:** None | | X | X |
| **IP.3 – Incident Recovery** | IP.3(1) – Recovery Plan | **CSF:** RC.RP-1, RC.CO-1, RC.CO-3<br>**NERC CIP:** CIP-009-6<br>**NIST SP 800-53R4:** CP-2, CP-10, IR-4, IR-8, SI-17 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **ESCSWG:** None<br>**Other:** NIST SP 800-61 | | | |
| | IP.3(2) – Review and Update Recovery Plan | **CSF:** RC.IM-1, RC.IM-2<br>**NERC CIP:** CIP-009-6<br>**NIST SP 800-53R4:** IR-8<br>**ESCSWG:** None<br>**Other:** NIST SP 800-61 | | X | X |
| | IP.3(3) – Recovery Plan Training and Awareness | **CSF:** PR.IP-10<br>**NERC:** CIP-009-6<br>**NIST SP 800-53R4:** CP-4, IR-3, PM-14<br>**ECSCSWG:** None | | X | X |
| **IP.4 – Incident Reporting** | IP.4(1) – Incident Reporting Policy | **CSF:** RS.CO-2<br>**NERC:** CIP-008-5<br>**NIST SP 800-53R4**: AU-6, IR-6, IR-8, SI-17<br>**ESCSWG:** None<br>**Other:** NIST SP 800-61 | | X | X |
| **Network Architecture and Security (NA)** | | | | | |
| **NA.1 – Network Design** | NA.1(1) – Design Baseline | **CSF:** DE.AE-1<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** AC-4, CA-3, CM-2<br>**ESCSWG:** 2.7 | X | X | X |
| | NA.1(2) – Least Functionality Configuration | **CSF:** PR.PT-3<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-005-5, CIP-007-6<br>**NIST SP 800-53R4:** AC-3, CM-6, CM-7<br>**ESCSWG:** 2.1 | X | X | X |
| | NA.1(3) – Firewalls | **CSF:** PR.PT-4, PR.AC-5<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-005-5, CIP-007-6<br>**NIST SP 800-53R4:** AC-4, AC-10, SC-7, AC-17, AC-18, CP-8, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC38, SC-39, SC-40, SC-41, SC-43<br>**ESCSWG:** 2.7 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| **NA.2 – Network Protection** | NA.2(1) – Network Communications | **CSF:** PR.PT-4<br>**NERC CIP:** CIP-004-6, CIP-005-5<br>**NIST SP 800-53R4:** AC-4<br>**ESCSWG:** 2.7 | X | X | X |
| **NA.3 – Network Detection** | NA.3(1) -Detection | **CSF:** DE.AE-2, DE.AE-3, DE.AE-4<br>**NERC CIP:** CIP-003-8, CIP-007-6, CIP-008-5<br>**NIST SP 800-53R4:** AU-6, CA-7, IR-4, IR-5, RA-3, SI-4<br>**ESCSWG:** 4, 4.1, 4.2 | X | X | X |
| | NA.3(2) – Alerts | **CSF:** DE.AE-5<br>**NERC CIP:** CIP-003-8, CIP-008-5<br>**NIST SP 800-53R4:** IR-4, IR-5, IR-8<br>**ESCSWG:** None | | X | X |
| **NA.4 – Network Monitoring** | NA.4(1) – Security Information and Event Management | **CSF:** DE.CM-1, DE.CM-6<br>**NERC CIP:** CIP-005-5<br>**NIST SP 800-53R4:** AC-2, AU-12, CA-7, CM-3, PS-7, SA-4, SA-9, SC-7, SI-4<br>**ESCSWG:** 2.6 | X | X | X |
| | NA.4(2) – Malware Detection | **CSF:** DE.CM-4<br>**NERC CIP:** CIP-003-8, CIP-007-6<br>**NIST SP 800-53R4:** SC-18, SC-44, SI-3, SI-8<br>**ESCSWG:** 2.8 | X | X | X |
| | NA.4(3) – Communicate Event Detection | **CSF:** DE.DP-4<br>**NERC CIP:**<br>**NIST SP 800-53R4:** AU-6, CA-2, CA-7, RA-5, SI-4<br>**ESCSWG**: None | | X | X |
| **NA.5 – Auditing** | NA.5(1) – Audit/Log Events | **CSF:** PR.PT-1<br>**NERC CIP:** CIP-006-6, CIP-007-6<br>**NFPA 800-53R4:** AU-2, AU-3, AU-8, AU-12<br>**ESCSWG:** 2.6 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | NA.5(2) – Audit/log Records | **CSF:** PR.PT-1<br>**NERC CIP:** CIP-006-6, CIP-007-6<br>**NIST SP 800-53R4:** AU-3, AU-4, AU-6, AU-9, AU-11<br>**ESCSWG:** 2.6 | X | X | X |
| | NA.5(3) – Audit Review, Analysis, Reporting | **CSF:** PR.PT-1<br>**NERC CIP:** CIP-006-6, CIP-007-6<br>**NIST SP 800-53R4:** AU-6<br>**ESCSWG:** 2.6 | X | X | X |
| **Physical and Environment (PE) Security** | | | | | |
| **PE.1 – Physical Security** | PE.1 (1) – Manage Access to Assets | **CSF:** PR.AC-2, PR.AC-3<br>**NERC CIP:** CIP-003-8, CIP-004-6, CIP-005-5, CIP-006-6<br>**NIST SP 800-53R4:** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8<br>**ESCSWG:** 5.1, 5.2 | X | X | X |
| **PE.2 – Manage Media** | PE.2(1) – Removable Media | **CSF:** PR.PT-2<br>**NERC CIP:** CIP-003-8, CIP-004-6 , CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8<br>**ESCSWG:** 2.8 | X | X | X |
| **PE.3 – Data Leakage** | PE.3(1) – Wireless Leakage | **CSF:** PR.PT-4, PR.DS-4<br>**NERC CIP:** CIP-003-8 , CIP-010-2<br>**NIST SP 800-53R4:** IA-2, SC-5, SC-23, SC-40, SC-43, SI-4,<br>**ESCSWG:** None | | X | X |
| | PE.3(2) – Physical Leakage | **CSF:** PR.AC-2<br>**NERC CIP:** CIP-003-5, CIP-004-5, CIP-006-5, CIP-010-2, CIP-011-2<br>**NIST SP 800-53R4:** PE-4<br>**ESCSWG:** 5.3<br>**Other:** BIMCO 5.2 | **X** | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| **PE.4 – Environment Management** | PE.4(1) – Manage Environment | **CSF:** PR.DS-7, PR.IP-5, DE.CM-2<br>**NERC CIP:** CIP-002-5.1a, CIP-003-8, CIP-005-5, CIP-006-6, CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** CA-7, CM-2, PE-3, PE-6, PE-10, PE-12, PE-13, PE14, PE-15, PE-18, PE-20<br>**ESCSWG:** 2.7, 6.1 | | | X |
| | PE.4(2) – Monitor Physical Environment | **CSF:** DE.CM-2<br>**NERC CIP:** CIP-006-6<br>**NIST SP 800-53R4:** AU-12, CA-7, PE-3, PE-6, PE-20<br>**ESCSWG:** 5.1 | X | X | X |
| **Cybersecurity Program Management (PM)** | | | | | |
| **PM.1 – Cybersecurity plan** | PM.1(1) – Cybersecurity Plan | **CSF:** ID.GV-1, ID.GV-2, ID.GV-4<br>**NERC CIP:** CIP-002-5.1a, CIP-003-8, CIP-004-6<br>**NIST SP 800-53R4:** PL-1, PL-2, PM-8<br>**ESCSWG:** None | X | X | X |
| | PM.1(2) – Maintenance of Cybersecurity Plan | **CSF:** ID.GV-1, ID.GV-2, ID.GV-4<br>**NERC CIP:** CIP-002-5.1a, CIP-003-8, CIP-004-6, CIP-007-6<br>**NIST SP 800-53R4:** PL-1, PL-2, PM-8<br>**ESCSWG:** None | X | X | X |
| **PM.2 – Cybersecurity Organization** | PM.2(1) – Roles and Responsibilities | **CSF:** ID.AM-6, ID.RM-3, PR.AT-2<br>**NERC CIP:** CIP-003-8, CIP-004-6<br>**NIST SP 800-53R4:** AT-3, CP-2, PS-7, PM-11, PM-8, PM-9, PM-11, PM-13, SA-14<br>**ESCSWG:** 2.2, 3.5 | X | X | X |
| **PM.3 – Cybersecurity Governance** | PM.3(1) – Legal and Regulatory | **CSF:** ID.GV-3, ID.GV-4<br>**NERC CIP:** CIP-008-6<br>**NIST SP 800-53R4:** AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-3, PM-7, PM-9, PM-10, PM-11, PS-1, RA-1, SA-1, SA-2, SC-1 | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **ESCSWG:** 3.3 | | | |
| **PM.4 – Cybersecurity Policies and Procedures** | PM.4(1) – Cybersecurity Policies and Procedures | **CSF:** ID.GV-1, ID.RM-1, ID.SC-1,<br>**NERC CIP:** CIP-002-5.1a, CIP-003-8, CIP-004-6, CIP-009-6<br>**NIST SP 800-53R4:** RA-2, RA-3, PM-9, -1 controls from all security control families<br>**ESCSWG:** 2.10, 3.1 | X | X | X |
| **PM.5 – Awareness and Training** | PM.5(1) – Training | **CSF:** PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-5<br>**NERC CIP:** CIP-003-8, CIP-004-6<br>**NIST SP 800-53R4:** AT-1, AT-2, AT-3, PS-7, SA-9, SA-16, PM-3<br>**ESCSWG:** 3.5 | X | X | X |
| | PM.5(2) – Training Records | **CSF:** PR.AT-4<br>**NERC CIP:** CIP-003-8, CIP-004-6<br>**NIST SP 800-53R4:** AT-3, PM-13<br>**ESCSWG:** 3.5 | X | X | X |
| **Cybersecurity Risk Management (RM)** | | | | | |
| **RM.1 – Mission Security** | RM.1(1) – Cybersecurity Objectives and Goals | **CSF:** ID-RA-3, ID.RA-4, ID.RA-5, ID.RA-6<br>**NERC CIP:** CIP-002-5, CIP-007-6, CIP-008-5, CIP-010-2<br>**NIST SP 800-53R4:** RA-2, RA-3, SA-14, SI-5, PM-4, PM-9, PM-11, PM-12, PM-16<br>**ESCSWG:** None | X | X | X |
| | RM.1(2) – Business Environment | **CSF:** ID.BE-1, ID.BE-2, ID.BE-3, ID.BE-4, ID.BE-5, ID.RM-2, ID.RM-3<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** CP-2, CP-8, PE-9, PE-11, SA-12, SA-14, PM-8, PM-9, PM-11<br>**ESCSWG:** None | X | X | X |
| **RM.2 – Security Standards** | RM.2(1) – Reliance and Adherence to Standards | **CSF:** DE.DP-2<br>**NERC CIP:** None | X | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **NIST SP 800-53R4:** AC-25, CA-2, SA-18<br>**ESCSWG:** 2.10 | | | |
| **RM.3 – Risk Assessments** | RM.3(1) – Vulnerability Assessments | **CSF:** ID.RA-1, ID.RA-3, ID.GV-4<br>**NERC CIP:** CIP-003-8, CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** RA-3, RA-5, PM-9<br>**ESCSWG:** 3.1, 3.2 | | X | X |
| | RM.3(2) – Vulnerability Management Plan | **CSF:** PR.IP-12<br>**NERC CIP**: CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** RA-3**,** RA-5, SI-2<br>**ESCSWG:** 3.1, 3.2 | X | X | X |
| | RM.3(3) – Vulnerability Scanning | **CSF:** DE.CM-8<br>**NERC CIP:** CIP-003-8, CIP-007-6, CIP-010-2<br>**NIST SP 800-53R4:** RA-5<br>**ESCSWG:** 3.1, 3.2 | | X | X |
| | RM.3(4) – Risk Assessment Process | **CSF:** ID.RA-5, ID.RA-6, ID.RM-2<br>**NERC CIP:** CIP-007-6, CIP-014-2<br>**NIST SP 800-53R4:** RA-2, RA-3, PM-4, PM-9, PM-16<br>**ESCSWG:** 3.1, 3,2, 3.3 | X | X | X |
| | RM.3(5) – Plan of Action and Milestones | **CSF:** ID.RA-6<br>**NERC CIP:** CIP-007-6, CIP-008-5, CIP-010-2<br>**NIST SP 800-53R4:** PM-4, SI-2<br>**ESCSWG:** 3.1, 3,2, 3.3 | x | X | X |
| **RM.4 – Supply Chain Risk Management** | RM.4(1) – Supply Chain Risk Management Policy | **CSF:** ID.SC-1, ID.SC-3<br>**NERC CIP:** CIP-013-1<br>**NIST SP 800-53R4:** SA-9, SA-11, SA-12, PM-9<br>**ESCSWG:** 3.2<br>**Other:** NIST SP 800-161 | X | X | X |
| | RM.4(2) – Suppliers and Third-Party Partners | **CSF:** ID.SC-2<br>**NERC CIP:** CIP-013-1 | | X | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **NIST SP 800-53R4:** SA-9, SA-10, SA-11, SA-12, SA-15<br>**ESCSWG:** 3.6<br>**Other:** NIST SP 800-161 | | | |
| | RM.4(3) – Delivery Protection | **CSF:** ID.SC-2<br>**NERC CIP:** CIP-013-1<br>**NIST SP 800-53R4:** SA-8, SA-9, SA-12, SA-18<br>**ESCSWG:** 3.6<br>**Other:** NIST SP 800-161 | X | X | X |
| | RM.4(4) – Periodic Audits | **CSF:** ID.SC-4<br>**NERC CIP:** CIP-013-1<br>**NIST SP 800-53R4:** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12<br>**ESCSWG:** 3.2<br>**Other:** NIST SP 800-161 | | X | X |
| **Security Development (SD) Practices** | | | | | |
| **SD.1 – Security Assessments** | SD.1(1) – Periodic Security Assessments | **CSF:** ID.RA-1; PR.IP-7, DE.DP-5<br>**NERC CIP:** CIP-007-6<br>**NIST SP 800-53R4:** CA-1, CA-2, CA-5<br>**ESCSWG:** 3.1 | X | X | X |
| | SD.1(2) – Security Testing | **CSF:** ID.RA-1, PR.IP-2, PR.IP-12, DE.CM-8<br>**NERC CIP:** CIP-007-5, CIP-010-1<br>**NIST SP 800-53R4:** PE-3, RA-5, SA-11<br>**ESCSWG:** 3.1 | | | X |
| **SD.2 – Security Alerts, Advisories and Directives** | SD.2(1) – Security Alerts | **CSF:** DE.DP-5<br>**NERC CIP:** CIP-008-5<br>**NIST SP 800-53R4:** SI-5, PL-2<br>**ESCSWG:** None | | X | X |
| | SD.2(2) – Threat intelligence | **CSF:** ID.RA-2<br>**NERC CIP:** None<br>**NIST SP 800-53R4:** SI-5, PM-15, PM-16 | | | X |

| Cybersecurity Best Practices | Best Practice Security Measures | Resources for Security Measures | Risk Level 1 | Risk Level 2 | Risk Level 3 |
|---|---|---|---|---|---|
| | | **ESCSWG:** None | | | |

**Pacific Northwest National Laboratory**

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

***www.pnnl.gov***