Pacific Northwest
NATIONAL LABORATORY

PNNL-29802

Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems

Revision 0

September 2020

Fleurdeliza A de Peralta
Alicia M Gorton
Mark Watson
Ryan M Bays
Jerry E Castleberry
Joshua R Boles
Brandon T Gorton
Ford E Powers

U.S. DEPARTMENT OF ENERGY

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

DISCLAIMER

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-29802

Framework for Identifying Cybersecurity Vulnerability and Determining Risk for Marine Renewable Energy Systems

Revision 0

September 2020

Fleurdeliza A de Peralta
Alicia M Gorton
Mark Watson
Ryan M Bays
Jerry E Castleberry
Joshua R Boles
Brandon T Gorton
Ford E Powers

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

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

Technology innovation, market demand, and the potential impacts of a changing climate are driving the marine renewable energy (MRE) industry to develop market-ready systems to provide low-carbon electricity for emerging, off-grid markets. 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 a predictable, affordable, and reliable source of energy from oceans and rivers, 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 controls 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 determining industry best practices to protect from those threats (Focus 2). This report provides the results of Focus 1 and describes a framework for determining the cybersecurity risk of an MRE system and its end use. The framework involves knowing the MRE system assets, network architecture, and operational configurations; the vulnerabilities that the assets will have to a cyberattack based on known threats to industrial control systems in the energy sector; and the consequences of a cyberattack on the end user. The resultant framework can be used by MRE developers and end users to determine their cybersecurity risk posture and implement appropriate security controls to mitigate impact and minimize the risk of a cyberattack on MRE systems. The results of Focus 2 are included in a supplement report, PNNL-30256, *Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems*, which identifies cybersecurity best practices commensurate with the risk level.

Summary

Marine renewable energy (MRE) encompasses forms of energy harnessed from the marine and riverine environment, including ocean tides, waves, currents, salinity gradients, temperature gradients, and riverine flows. Technology innovation, market demand, and the potential impacts of a changing climate are driving the MRE industry to develop market-ready devices to power certain off-grid markets (e.g., desalination facilities, ocean observation, underwater vehicle charging, and isolated coastal communities). The advanced operational and information technology used in MRE system designs expands the attack surface for cyber-threat actors with malicious intent to gain unauthorized access to data or disrupt operation of the energy-generating device. The U.S. Department of Energy is committed to protecting the electric power infrastructure by focusing on cybersecurity of energy-generating assets. Thus, the Water Power Technologies Office within the Office of Energy Efficiency and Renewable Energy 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.

This report addresses the first focus area, which describes the framework to identify cybersecurity vulnerabilities of an MRE system and its end use and assess the consequences of a cyberattack to determine the cybersecurity risk. The framework addresses information on typical MRE assets and known cyber threats to the energy sector and industrial control systems. MRE system stakeholders can use the risk model to identify known threats, the likelihood of vulnerabilities, and evaluate consequences of a cyber incident to determine a cybersecurity risk level.

Three different risk levels were modeled in this report. The risk levels reflect a graded approach to manage cybersecurity vulnerabilities based on a qualitative assessment of the likelihood of cybersecurity threats and the impact a cybersecurity attack would have on the MRE system and end use. The graded approach provides MRE system owners flexibility to ascertain the necessary cybersecurity to prevent and mitigate a potential cyberattack. The second focus area is addressed in the Pacific Northwest National Laboratory Report PNNL-30256, *Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems*, which describes the MRE system risk management framework and identifies risk-based industry cybersecurity best practices tailored to protect MRE systems.

Acknowledgments

Pacific Northwest National Laboratory thanks Dr. Mark Christian and the Water Power and Technologies Office within the Office of Energy Efficiency and Renewable Energy for the U.S. Department of Energy for his dedicated support. Pacific Northwest National Laboratory also acknowledges and thanks the marine renewable energy system developers and other key stakeholders that provided information on the design and operation of their devices when deployed for various end users. This information helped the research team determine the specific types of cyber threats and vulnerabilities for marine renewable energy systems. Pacific Northwest National Laboratory also thanks Miles Hall and the members of the Marine Energy Council for communicating our research to marine renewable energy stakeholders and for sharing their experience with marine renewable energy system designs and operations.

Acronyms and Abbreviations

ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
ICS	industrial control system
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IT/OT	Information technology and operation technology
MHK	Marine Hydrokinetic
MRE	marine renewable energy
NIST	National Institute of Standards and Technology
OCS	Outer Continental Shelf
PNNL	Pacific Northwest National Laboratory
RMF	Risk Management Framework
SP	Special Publication
WPTO	Water Power Technologies Office

Contents

Figures

Tables

1.0 Introduction

Marine renewable energy (MRE) encompasses forms of renewable energy that can be harnessed from the marine and riverine environments, including ocean tides (tidal energy), waves (wave energy), currents (ocean current energy), salinity gradients, and temperature gradients (ocean thermal energy conversion), along with riverine energy[1]. The U.S. Department of Energy (DOE) Water Power Technologies Office (WPTO) has conducted resource assessments for wave, tidal, ocean current, and riverine energy, as shown in Table 1. The theoretical resource potential is the annual average amount of physical energy that is hypothetically available, while technical resource potential is the portion of the theoretical resource that can be captured using a specific technology.

Table 1. U.S. MRE Resource Potentials [1]

Resource Assessment	Resource Potential
Waves	Theoretical: 1,594–2,640 TWh/year Technical: 898–1,229 TWh/year
Tidal streams	Theoretical: 445 TWh/year Technical: 222–334 TWh/year
Ocean currents	Theoretical: 200 TWh/year Technical: 45–163 TWh/year
River currents	Theoretical: 1,381 TWh/year Technical: 120 TWh/year

To date, little has been done to connect MRE to the grid [2], although there are hydrokinetic tidal and river projects that demonstrated the ability to connect to a utility grid and a local microgrid, respectively [33,34]. Technology advancement for MRE integration with the grid is challenged by long design and development (develop, test, refine, and iterate) cycles that often take years, application in dynamic and extreme environments, and long permitting cycles [3]. However, technology innovation and increased market demand for renewable energy sources are driving the MRE industry to develop market-ready devices for MRE beyond the grid. Solutions for both legacy and emerging industries (e.g., desalination, underwater vehicle recharging) could be developed and accelerated by aligning recent advances in MRE technology with the “blue economy” [3,4]. Industry clusters are beginning to form around maritime “blue” technologies that could be powered by harnessing the energy associated with ocean waves and tides, recognizing the engineering, regulatory, operational, and market challenges associated with ocean development [3]. The threat of cybersecurity attacks within analogous industries, such as maritime transportation [6], the energy grid industry [7], and the overall renewable energy industry [7], is attracting more attention. Today’s nascent MRE industry is well positioned to begin investigating cybersecurity architecture designs and risk assessment approaches, while many MRE technologies are in early stages of research and development, and many of the blue economy markets are still emerging and/or maturing.

[1] For the purposes of this guidance, only wave, tidal, ocean current, and riverine energy are considered.

To provide a level of assurance that MRE systems are a viable, resilient, and secure power resource for specialized markets (e.g., desalination facilities, ocean observation, underwater vehicle charging, isolated coastal communities.), DOE WPTO has funded Pacific Northwest National Laboratory (PNNL) 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 the cybersecurity risks.

This report addresses the first focus area and describes the framework that MRE stakeholders can use to assess the vulnerabilities and cybersecurity risk of information technology and operational technology (IT/OT) systems and interconnections with their end users.

Section 2.0 of this report provides the background of the MRE industry and how development of a cybersecurity guidance will improve its resiliency as a reliable source of energy.

Section 3.0 describes the approach used to evaluate the cybersecurity vulnerabilities and risks of an MRE system and its end use.

Section 4.0 describes the results of the research, including the different IT/OT systems and communication methods used by MRE systems, the types of cybersecurity threats and their consequences, and a method to determine the cybersecurity vulnerability and risk to the system and its end users.

Section 5.0 summarizes the framework that MRE system owners and operators can use to evaluate cybersecurity risk.

2.0 Background

This section describes the energy sector's cybersecurity policy, provides an overview of MRE systems, and describes how cybersecurity policy and threats apply to MRE systems.

2.1 Cybersecurity Policy for the Energy Sector

Recognizing that MRE development is maturing and near-term markets are emerging, WPTO and the DOE Office of Energy Efficiency and Renewable Energy understand the growing need to identify and mitigate cybersecurity threats in this space. Thus, as a part of congressional appropriation, Energy Efficiency and Renewable Energy technology offices were tasked with enabling MRE cybersecurity guidance. Creating cybersecurity guidance for MRE devices allows developers to address cyber risks and implement mitigations into the development life cycle, giving the capability for robust compensatory measures. Incorporating cybersecurity risk mitigation capabilities into the design of the MRE device and system is paramount to the protection of energy generation and any enterprise networks that are interfaced.

On November 16, 2018, the U.S. Department of Homeland Security established the Cybersecurity and Infrastructure Security Agency (CISA) as promulgated by the Cybersecurity and Infrastructure Security Act of 2018.[2] CISA provides cybersecurity and infrastructure security knowledge and best practices to various stakeholders to protect our nation's essential resources. CISA was also established to work with different federal civilian department and agencies to adopt common polices and best practices to protect against cyber threats and thus integrates similar functions performed by the U.S. Computer Emergency Readiness Team and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). These functions include risk intelligence, threat mitigation and vulnerability awareness through advisories and alerts.

DOE has a substantial interest in reducing cybersecurity risks and increasing the resilience of new and existing energy-generating devices. Cyber-attacks on energy control systems could result in significant disruption to operations and national security. Therefore, it is paramount that the energy sector develops and applies cybersecurity standards, policies, and procedures. The National Institute of Standards and Technology (NIST) makes available frameworks for both public and private organizations requiring robust security measures. NIST has a leading role in how DOE structures its cybersecurity program and includes minimum standards, benchmarks, and implementation guidelines as they relate to cybersecurity. The energy sector worked with NIST to develop the Energy Sector Cybersecurity Framework Implementation Guidance [8], which was designed to protect reliable means of energy from cyber-attacks by aligning the needs of the energy sector with the requirements of the NIST Cybersecurity Framework (CSF) to establish protections needed for critical infrastructure [21]. This framework serves as a foundation to the fundamental strategies of the energy sector's cybersecurity mission and includes the five functions of the NIST Framework: identify, protect, detect, respond, and recover.

The DOE Office of Energy Efficiency and Renewable Energy has adopted a holistic approach to the cyber-physical threat landscape to minimize attack vectors and cyber vulnerabilities. The

[2] Cybersecurity and Infrastructure Security Act of 2018 https://www.congress.gov/bill/115th-congress/house-bill/3359

DOE Office of Energy Efficiency and Renewable Energy produced the Energy Sector Cybersecurity Framework Implementation Guidance [8], which implements the fundamentals of the NIST standards and functions to promote robust cyber-physical governance that is tailored to provide reliable means of energy production.

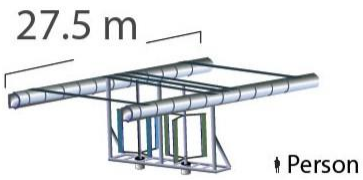
2.2 Overview of MRE Systems and End-Use Markets

The MRE systems under the purview of this guidance include wave, tidal, ocean current, and riverine energy devices and are understood broadly as:

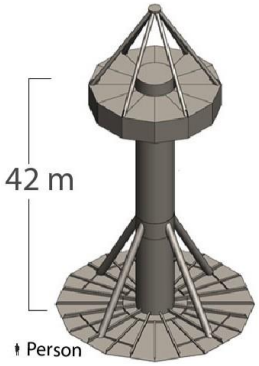
- **Tidal current devices**: devices that harness energy from flow of tidal currents [10] (e.g., tidal current turbine; Figure 1a)
- **Riverine energy devices**: devices that harness the kinetic energy from flowing waters in rivers[3] (e.g., river current turbine; Figure 1b)
- **Wave energy converters**: devices that harvest the kinetic and potential energy from ocean waves [9] (e.g., wave point absorber; Figure 1c)
- **Ocean current energy devices**: devices that harness the horizontal flow of ocean currents that are generated and affected by meteorological and oceanographic conditions [2] (e.g., ocean current turbine; Figure 1d)
- **Oscillating surge flap:** A type of floating and oscillating surge wave energy converter that harnesses energy from the surge motion of waves to generate electrical power [32] (Figure 1e).
- **Oscillating water column:** A type of wave to pneumatic energy converter that harnesses energy from the oscillation of seawater inside a chamber or hollow caused by the action of waves (Figure 1f).

Figure 1 includes illustrations of six “reference models” of MRE devices 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 levelized costs of energy) [11, 32]. 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

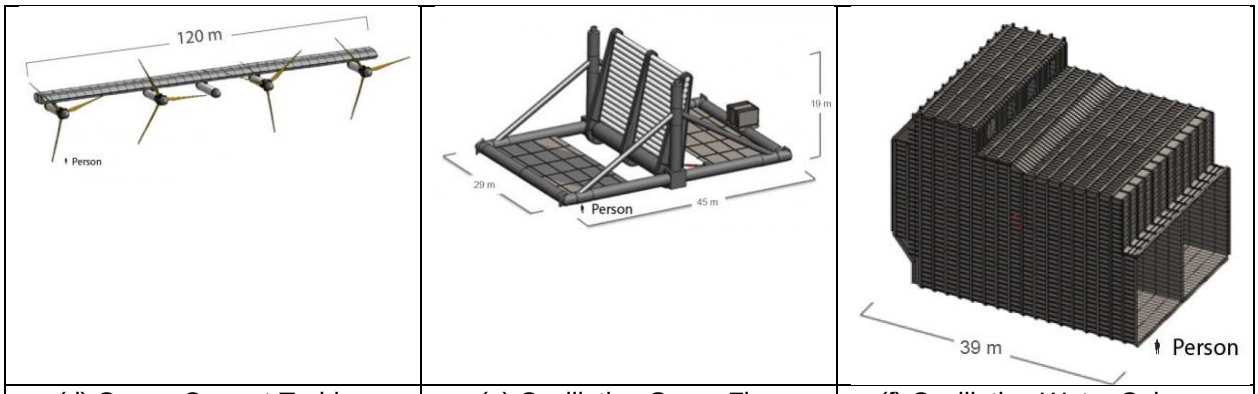


(b) River Current Turbine



(c) Wave Point Absorber

[3] https://tethys-engineering.pnnl.gov/technology/riverine. Accessed on March 9, 2020



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

Figure 1. Illustrations of MRE Reference Models [11]

DOE WPTO is investing in MRE technology development to drive innovation within the industry to develop market-ready devices for MRE applications beyond the grid. The rapid growth of the emerging blue economy has prompted DOE WPTO to explore non-grid opportunities for MRE within emerging blue economy markets where MRE may provide advantages and solutions to energy limitations (Figure 2) [3].

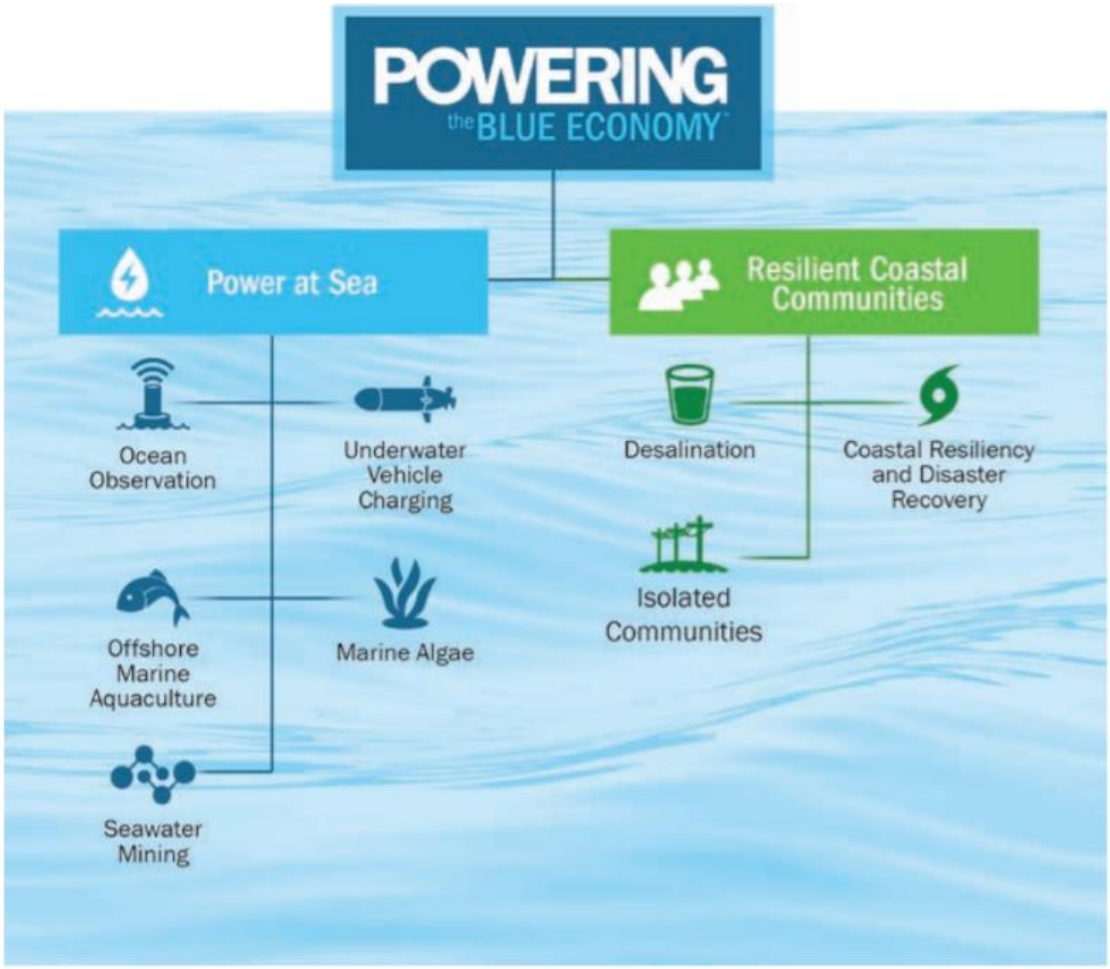
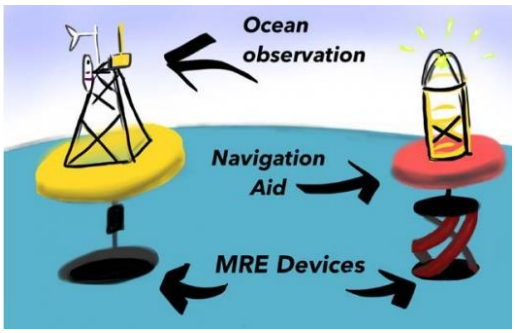


Figure 2. Potential Marine Power Applications within the Blue Economy

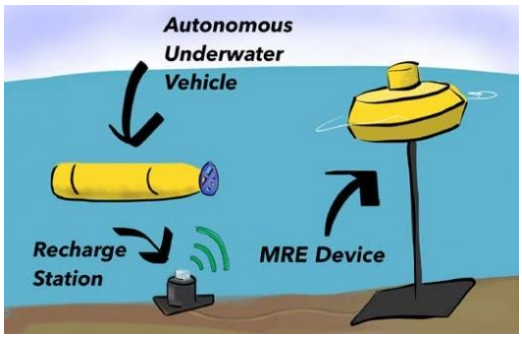
The applications are divided into two areas: Power at Sea and Resilient Costal Communities [3].

- **Power at Sea**: using MRE 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 [3], where the delivery of power can be expensive and challenging. For example, offshore marine hydrokinetic project on the Outer Continental Shelf would likely implement wave- or ocean-current-based MRE technologies [23] (such as wave-point absorbers or ocean current turbines) to power marine applications and devices at sea.
- **Resilient Coastal Communities**: using MRE to support coastal communities and facilities, increasing resilience when faced with extreme events such as tsunamis, hurricanes, or floods. 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.

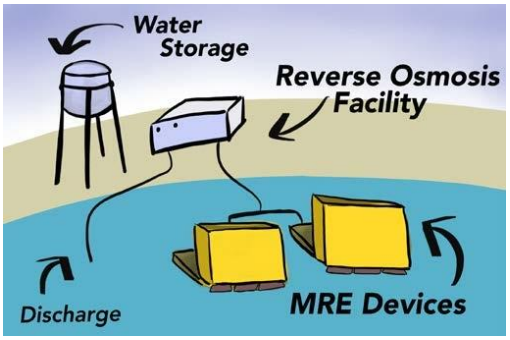
Figure 3 shows four blue economy markets that DOE WPTO identified to have potential near-term opportunities for MRE integration based on market maturity and readiness. First, MRE has the potential to power ocean observation and navigation systems, where battery capacity, data storage, and transmission to shore often limit operations. Second, underwater charging and docking stations for underwater vehicles can potentially be powered by MRE, as battery-power capability often limits mission duration. Third, coastal desalination facilities that provide drinking water to communities can potentially receive power from nearshore MRE systems. Finally, MRE systems may also provide electricity to remote, isolated communities dependent on diesel fuel.



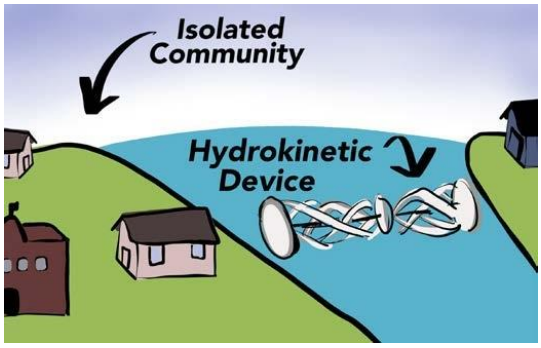
(a) Ocean observation and navigation



(b) Underwater vehicle recharging



(c) Desalination



(d) Isolated power systems

Figure 3. Near-Term Blue Economy Markets [3]

Error! Not a valid bookmark self-reference. includes additional information on each of the four near-term markets, including a description of the market and potential end users. Additional details on the four near-term markets and the additional markets not explicitly discussed herein are provided in [3].

Table 2. Near-Term Blue Economy Markets [3]

Power at Sea	
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 (Figure 3a)	
Ocean Observation • National Oceanic and Atmospheric Administration – National Data Buoy Center – Pacific Marine Environmental Laboratory – Integrated Ocean Observing System – Regional ocean observation systems • U.S. Coast Guard • U.S. Department of Defense (DoD) – U.S. Navy – U.S. Defense Advanced Research Projects Agency	Navigation • U.S. Coast Guard • U.S. Army Corps of Engineers • National Oceanic and Atmospheric Administration Coastal Survey • 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 (Figure 3b)	
• DoD – U.S. Navy – Defense Advanced Research Projects Agency • U.S. Department of Homeland Security • National Oceanic and Atmospheric Administration – Integrated Ocean Observing System – Regional ocean observing systems	
Resilient Coastal Communities	
Desalination	
Provide power to coastal desalination facilities that provide drinking water to communities (Figure 3c)	
• Municipalities already deploying or building desalination facilities to mitigate drought or water security risks	
Isolated Power Systems	
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 (*Figure 3d*)	

- Remote/islanded or isolated communities or resorts that have microgrid power systems
- DoD
  - Defense Advanced Research Projects Agency
  - Environmental Security Technology Certification Program
  - Strategic Environmental Research and Development Program
  - Energy Resilience and Conservation Investment Program

2.3 Overview of Cybersecurity Incidents

The threat landscape facing current and future industrial control systems (ICSs) carries with it the possibility of MRE systems being faced with similar cyber incidents. The development of cybersecurity guidance will enable the MRE industry to design and operate the energy delivery functions and continue performing critical functions during and after a cyberattack.

The need to secure electronic information has remained constant throughout the evolution of the digital age. Initially, threats were isolated to individual networks comprised of like devices and users. With the proliferation of network connectivity and the development of new, user-demanded capabilities (e.g., remote access, data visualization, system integration), risks have grown exponentially to span economic markets, geographic regions, and national boundaries. Threats, and the cybersecurity incidents they cause, have steadily increased because of these and other factors. Specific to critical infrastructure, a field of technologies in which renewable energy platforms are often included, cyberattacks targeting ICSs are becoming more common each year [13]. In particular, 35% of the critical infrastructure cyber incidents reported to ICS-CERT between 2013–2015 involved the energy sector [7].

The cyberattack on the Ukrainian power grid on December 23, 2015 resulted in loss of power for 225,000 customers and affected three different electric utilities. Cyber threat actors used spear phishing emails to gain access to IT networks and, once inside, stole credentials using keystroke loggers, identified hosts and devices, and hijacked the distribution management system to systematically open breakers and cause the power outage [7]. The ICS network was accessed through the virtual private network, and attackers disabled the uninterruptible power supply, disabled operational control systems, disabled computers, and prevented infected computers from rebooting. Attackers then used similar malware a year later to target remote power transmission facilities and cause another outage that lasted an hour. These events demonstrated how a cyberattack could involve long-term reconnaissance operations and execute a synchronized attack on multiple sites.

Common impacts of a cyberattack include theft of information/data, disruption to operations, potential impact to human safety, damage to reputation from customers/stakeholders, financial losses due to recovery from the incident, and fines and penalties to regulators. Malware can compromise a safety system by changing set points on the process controller and result in the process shifting to an unsafe condition [12].

Threats common to IT/OT systems and cyber-physical systems were evaluated to determine their applicability to MRE systems. The different uses and interconnectivity methods for MRE systems were also reviewed to determine cybersecurity vulnerabilities and risk.

3.0 Approach

In the United States, the Federal Energy Regulatory Commission under the authority of the Federal Power Act[4] [13] has jurisdiction over marine and hydrokinetic[5] projects on navigable waters (approximately within three nautical miles of shore) and over any projects with an onshore grid connection. 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 [31]. The Marine and Hydrokinetic Renewable Energy Act further stipulates that pursuant to Part I of the Federal Power Act, the Federal Energy Regulatory Commission authorizes and regulates nonfederal hydropower projects [30]. As such, cybersecurity for MRE systems and their end use are 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]. However, a DOE priority 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]. Owners and operators of MRE systems have the primary responsibility for managing cybersecurity risks. Consistent with the core functions of the NIST Cybersecurity Framework (Figure 3), the energy sector's continuous risk management functions require owners and operators to identify assets, protect critical systems, detect incidents, respond to incidents, and recover to normal operations.[7]

Figure 4. NIST Cybersecurity Framework Core Functions

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.

[4] Federal Power Act is described in Title 16 U.S. Code Chapter 12 – Federal Regulation and Development Power. https://legcounsel.house.gov/Comps/Federal%20Power%20Act.pdf
[5] Marine energy and hydrokinetic energy are often used interchangeably with MRE.

The NIST CSF was developed in 2014 as a result of collaboration between the private sector and government to manage cybersecurity risk across critical infrastructure sectors. However, NIST Special Publication (SP) 800-37, *Risk Management Framework for Information Systems and Organizations* [5], was developed in 2010 and has been mandatory for use by federal agencies. The NIST Risk Management Framework (RMF) describes a process for managing cybersecurity risk. The NIST CSF is incorporated into the NIST RMF, and the two different frameworks complement each other.

Because federal agencies and private industry have deployed MRE systems to support their mission, the cybersecurity program for those MRE systems could follow NIST RMF. To enable a consistent application of cybersecurity best practices for MRE systems, a framework similar to NIST SP 800-37 would be beneficial for owners and operators. Figure 5 describes the RMF for the MRE industry, which involves six steps that are continuously followed throughout the life cycle of the MRE system.

Figure 5. Marine Renewable Energy Systems Risk Management Framework

MRE system owners and operators should develop and manage their cybersecurity program using the RMF during initial deployment and daily operations throughout its life cycle. The six steps of the MRE Systems Cybersecurity RMF provide guidance on implementing a risk-based cybersecurity program.

- Step 1 determines the cybersecurity risk of an MRE system (e.g., Risk Level 1, 2, or 3) as discussed in Section **Error! Reference source not found.** of this report.
- Step 2 selects the security best practices commensurate with the risk, as described in PNNL Report PNNL-30256, *Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems*, [27].
- Step 3 implements the security measures to protect the systems and organization.
- Step 4 works 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 address 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, 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 (**Error! Reference source not found.**) during initial deployment and daily operations throughout its life cycle.

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 internet of things and industrial internet of things. The use of these technologies relies on interconnectivity and communication methods that enable potential security vulnerabilities that are leveraged by threat actors and hacktivists alike. This ultimately increases the risk to operations affected by a cyberattack.

This report describes an approach to determine the cybersecurity risk of the MRE system and its end use (Step 1 of the MRE System RMF). A supplemental report includes the guidance for the remaining steps 2 through 6 of the MRE system RMF.

The general approach to determine cybersecurity risk is twofold: collect information on the MRE system and operation and perform a cybersecurity risk analysis on the configuration. The following subsections describe the specific methods used to complete the two tasks. Section 4 discusses the results of completing the two tasks.

3.1 Collect Information on MRE Systems and Applications

To understand the business drivers and security vulnerabilities for MRE systems, information was collected from MRE developers and on the designs, operations, and end use of these systems from open source materials, such as the Portal and Repository for Information on Marine Renewable Energy[6]. The information collected identified categories of assets and communication methods that are susceptible to known cyber threats to ICS and energy sectors.

Typical assets in MRE system designs that would be susceptible to a cyberattacks include those that involve generating, storing, processing, and transmitting data, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. These types of assets are used to control and manage data related to operation of systems and would rely on technology to communicate the data to plant owners and operators to allow operators to remotely access the data and make informed operational decisions. These types of advanced technology involve low-cost internet protocol devices that have replaced proprietary control protocols, which have resulted in increased cybersecurity vulnerabilities and incidents.

The methods of communication also have associated cybersecurity vulnerabilities. For example, offshore MRE systems may communicate to remote operations using fiber optic cables that connect the MRE system assets to local area networks. Advanced technology may also involve the use of wireless networks or Bluetooth devices to interconnect devices, such as sensors and software applications that analyze data.

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

3.2 Perform Cybersecurity Risk Assessment

To assure appropriate security controls are implemented for the MRE assets and end use, owners and operators need to determine their susceptibility to a cyberattack. Figure 1 describes the elements used to perform a cybersecurity risk assessment to determine the cybersecurity risk posture for the MRE system and its configuration.

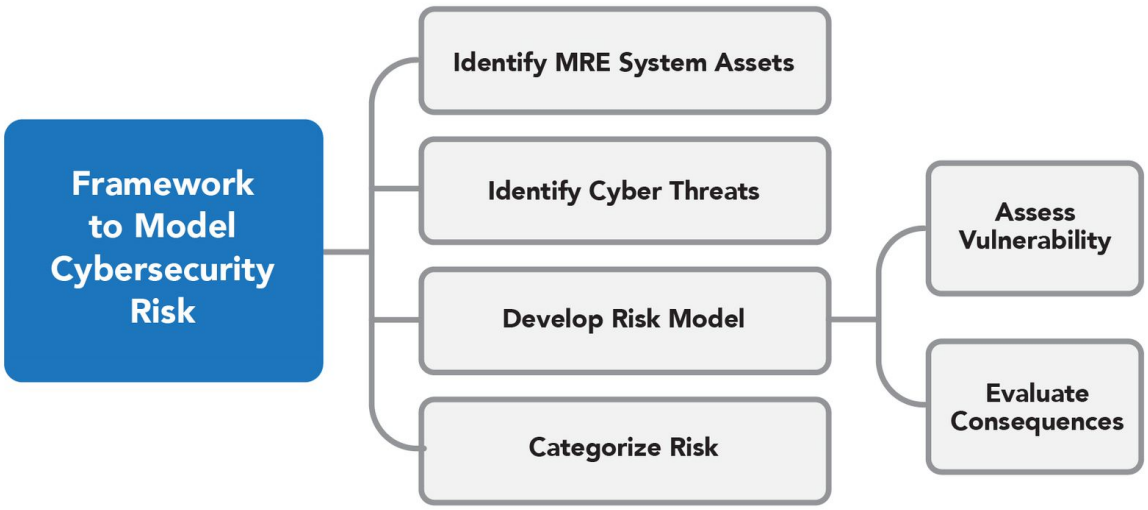


Figure 6. Framework to Model Cybersecurity Risk of an MRE System

The elements in the framework that determine the cybersecurity risk include identifying assets that are prevalent in MRE systems and their operation, determining prevalent threats, assessing the vulnerability of the MRE system assets, analyzing the likelihood of the threats, and evaluating the consequences to develop the risk model that will determine categorization of different MRE systems and their end uses. The specific approach used to complete each of the elements is described further in the following subsections, and the results are described in Section 4.

3.2.1 Identify MRE System Assets

A taxonomy of the MRE system assets was developed based on the information collected on MRE system design, operations, network architecture, expected communication methods, and intended application or end use. As shown in Figure 7, cyber threat actors could attack the MRE system components through different attack vectors. The purpose of this task is to identify the different assets and to segment them into hierarchical functions to perform the next step of identifying the types of threat vectors that should be considered in the analysis.

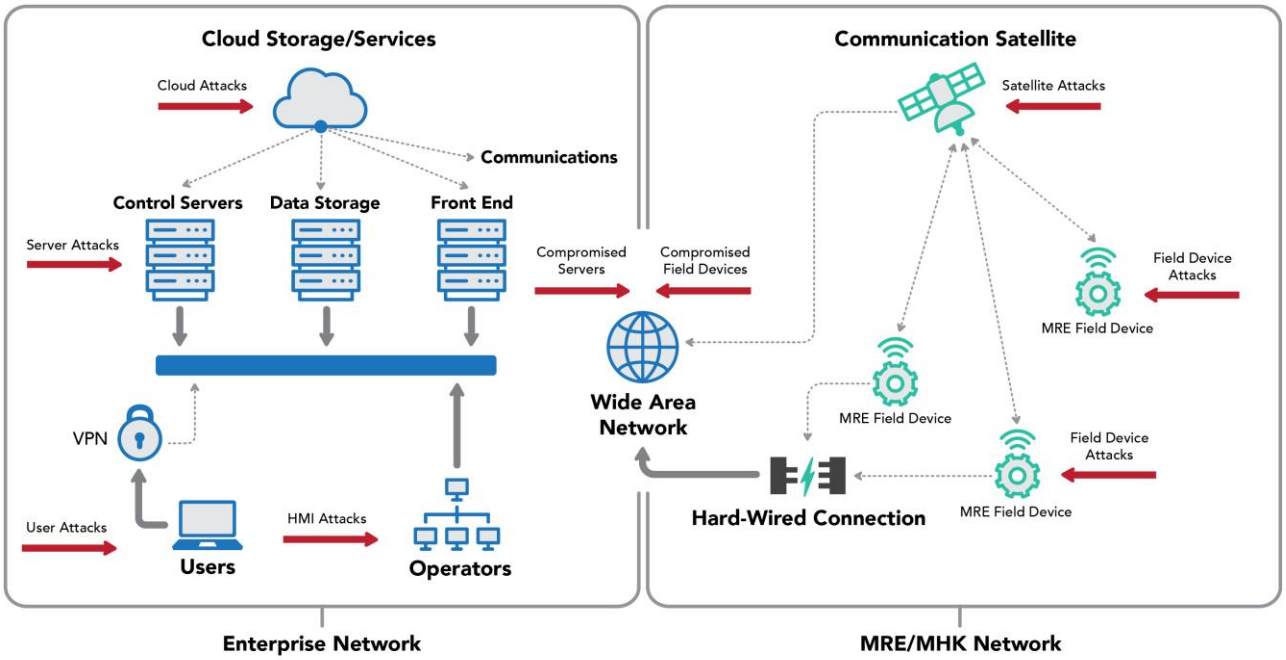


Figure 7. Example Attack Pathways into a Network Architecture

3.2.2 Identify Applicable Cybersecurity Threats

Many open sources identify cyber and cyber-physical threat and their attack vectors. This task identified cyber threats that are prevalent in the energy industry, industrial control systems, and MRE system assets. The types of cyber and physical threats were obtained from energy industrial control system reports, such as MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)) Matrix [18, 19, 20, 23] and ICS-CERT [17].. These threats were analyzed further to determine the most prevalent types of cyber threats that could attack MRE system assets.

3.2.3 Develop Cybersecurity Risk Model

New types of cyber threats are constantly discovered, which makes calculating the risks of a cybersecurity attack difficult. In addition, the likelihood that a vulnerability exploited by the success of a cyber threat is dependent on the level of cybersecurity that an organization implements. The right security implemented for the IT/OT networks for an MRE system can significantly secure and protect the system and reduce the likelihood of a cyberattack from a potential cyber threat actor. The challenge for the MRE system owner/operator is knowing the extent of security controls to implement that will be adequate with respect to the impact to its operation and business (i.e., enterprise, financial, interruption, etc.).

The cybersecurity risk to an MRE system is based on the likelihood that a cyber threat will exploit a vulnerability and the consequence to the MRE system and/or end use if a cyberattack occurs. The approach used to determine the likelihood of a vulnerability, cyber threat, and the consequences of a cyberattack are described further in the following subsections.

3.2.3.1 Assess Vulnerability of MRE Assets

The likelihood of a cybersecurity threat is dependent on a vulnerability and the protection provided on the digital assets. Other considerations that contribute to the likelihood are geography (i.e., offshore, nearshore, deep water, shallow water, etc.), accessibility to the MRE system and proximity from external sources, and interconnections with other external networks or organizations. Quantifying the likelihood of the cyber threat is not as straightforward as quantifying the impact that a cyberattack can have on the MRE system's operation and end user's business (e.g., loss of power, loss of operation, etc.). To simplify determining the likelihood of a cyber threat, a qualitative approach was used and considered the type of digital assets, geography, accessibility, and interconnectivity to other external networks.

3.2.3.2 Evaluate Consequences of Cyberattack

The impact of a cyberattack on the MRE systems is based on the end use of the MRE systems and the consequence on the end user's mission. The power generated by MRE systems has various end uses (e.g., grid integration, ocean observation, underwater vehicle charging, navigation aids, powering desalination plants, and coastal communities). The consequences of a cyberattack on the MRE system's end use was evaluated to determine how they affected the following:

- Interruption to business/mission
- Impact to safety
- Type of information/data loss (i.e., classified, controlled unclassified, etc.)
- Financial loss
- Potential to affect external networks due to its interconnectivity configurations (i.e., enterprise networks)

The consequences may vary between different owners and operators for the same type of MRE design. Thus, the risk is dependent on the impact to the stakeholder's mission.

3.2.4 Categorize Risk

Based on the likelihood of a cyber threat and the criteria for determining consequences, a cybersecurity risk model was developed for MRE systems and their end use. The model describes the qualitative cybersecurity risk based on the potential likelihood of occurrence of a cybersecurity threat to the MRE digital assets and the consequences on their end use.

A risk-based model allows the MRE system owner and operator to decide on the appropriate security that should be implemented. A progressive approach allows the owner and operator to prioritize the layers of defense-in-depth protection of MRE system assets commensurate with the cybersecurity risks of the MRE systems and their end uses. Defense-in-depth protection involves a series of security controls that are layered to protect data and information such that intentional redundancies in security increase the security as a whole and mitigate different attack vectors.

4.0 Results

4.1 MRE System Applications

Table 2 identifies some MRE end uses and is supplemented by information provided by MRE stakeholders in Requests for Information and from open research. The end users vary from different federal agencies, such as DOE, DoD (U.S. Navy, Army Corps of Engineers, Defense Advanced Research Projects Agency), Federal Energy Regulatory Commission, National Oceanic and Atmospheric Administration, U.S. Coast Guard, U.S. Department of Homeland Security, and Bureau of Ocean Energy Management, to non-federal agencies, such as utilities (private and public) under compliance and monitoring of the North American Electric Reliability Corporation Reliability Standards[7], testing centers, and research laboratories. Cybersecurity governance of MRE systems will be determined by their authoritative agency or requirements.

The MRE cybersecurity guidance aligns with the NIST CSF, NIST RMF, and DoD RMF. As a result of the Cybersecurity and Infrastructure Security Agency Act of 2018, CISA was established to adopt common polices and best practices to protect different federal civilian department and agencies against cyber threats. Federal agencies are required to follow the NIST CSF and NIST RMF. CISA also identified how different states govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. [14] The authority for establishing risk management standards and policies lies within the different state-level roles; however, the authority for identification and mitigation will vary from state to state. MRE systems deployed to support DoD missions will be governed by DoD's cybersecurity requirements, including the DoD RMF [25, 26].

4.2 MRE Cybersecurity Risk Model

The MRE cybersecurity risk model is developed following the guidance of the first NIST CSF core function, which identifies the cybersecurity risk to the MRE system (i.e., assets, data, operations, etc.) and its end user (i.e., organization, mission, capabilities, etc.). This core function is the foundation for understanding the end use context, the resources available to support cybersecurity, and the risks enabling the MRE stakeholder to prioritize a risk management strategy commensurate with the business needs of the end user. The risk model is based on information on MRE system assets, known threats to these assets, vulnerabilities to the assets, and the consequences to the MRE system and end user. Each risk model element is discussed in the following subsections.

4.2.1 MRE System Assets

MRE systems are expected to house networks as a platform to perform large amounts of data collection and in some cases data processing and transmission. As a result, many different types of digital components will make up the comprehensive MRE system.

MRE developers and key stakeholders (including test centers) provided non-sensitive and non-proprietary information on MRE system design, operations, network architecture, communication methods, and intended application or end use in response to a Request for Information questionnaire (Appendix C).

[7] North American Electric Reliability Corporation Reliability Standards. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

Based on the information received from the Portal and Repository for Information on Marine Renewable Energy,[8] MRE developers, and MRE test sites, a select number of assets (e.g., hardware, software, computer networks, communication methods, applications, and other IT/OT assets) are 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 **Error! Reference source not found.** and need to be protected from cyber-threat actors.

Table 3. Typical Assets on an MRE System

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

MRE developers also 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.

MRE system assets and information management methods were assessed further to ascertain the different threats and vulnerabilities that could apply to MRE systems specifically. In this way, the scope of the threat analysis is narrowed to a specific and useful size. According to research

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

from ICS-CERT and threat tracking groups like Dragos, the above listed assets have been the target of cyber threat actors within the ICS and energy sector industries.

4.2.2 Cybersecurity Threats Analysis

Cybersecurity threats specific to the renewable energy sector, particularly for MRE assets, have not been widely investigated and published. The potential cyber threats analyzed were based on the context of conventional MRE designs (Figure 1), information provided by stakeholders through the Request for Information, and available open source information by both public and private ICS industry cybersecurity leaders, such as ICS-CERT, Dragos, and MITRE.

The National Cybersecurity and Communications Integration Center was established in 2009 and is our nation's source for cyber and communication information, technical expertise, and operational integration. The National Cybersecurity and Communications Integration Center offers information to enhance situational awareness, analysis, incident response, and collaborates with ICS-CERT in communicating control-systems-related security incidents and mitigation measures to both public and private partners. In 2015, the Department of Homeland Security issued National Cybersecurity and Communications Integration Center/ICS-CERT Industrial Control Systems Assessment Summary Report, identifying common ICS cyber weaknesses, with the most common being insufficient network boundary protection [17]. An insufficient method of monitoring and controlling communications at the ICS network boundaries can contribute to unauthorized access into ICS and enterprise networks. Other common weaknesses in security controls include the following:

- Not establishing "least functionality" for systems could create threat vectors for unauthorized access to critical systems by malicious parties or rogue access by internal parties.
- Poor authentication management could compromise unsecured password communications and allow unauthorized access to systems.
- Lack of or weak identification and authentication controls could result in password compromise or repudiation of user actions. Not establishing "least privilege" could allow more authorized users with elevated privileges, resulting in larger attack surface for intruders to steal account credentials and elevate privileges.
- Poor allocation of resources can impede cybersecurity monitoring and response capability to a cyber incident.

Dragos issues *Year in Review* reports that provide insights and lessons learned on ICS incidents, including vulnerabilities, ICS landscape and threat activity groups, and lessons learned from the front lines of ICS cybersecurity. The 2019 *Year in Review* report identified increasing threat activity from adversaries targeting North American electric entities and growing ICS-specific threat landscape [18]. Some key findings in the 2019 *Year in Review* report included:

- Increased focus on ICS organizations, specifically in critical infrastructure across the United States
- Increasing third-party and supply chain threats to telecommunications, managed service providers, and internet service providers
- Ransomware and commodity malware remain threats to industrial operations and could potentially bridge the IT/OT gap to disrupt operations

- Popular common attack tactics, such as phishing, password spraying, and watering hole attacks that target specific groups, continue as effective initial access vectors
- Increased targeting of remote connectivity, such as virtual private networks, vendor and business management integrations, remote desktop connections, and managed service providers
- Increased likelihood that cyber threats will target ICS due to escalating geopolitical tensions

MITRE's ATT&CK matrix can be used as a source to determine if cybersecurity protection is adequate to detect and block certain types of attacks. The ICS-specific ATT&CK matrix provides information about cyberattack techniques used by adversaries against ICSs, the types of malware used against ICSs, threat groups known to launch ICS-related attacks, and the types of assets that can be targeted [19]. The assets that are commonly found in ICS can vary from Windows workstations specializing in applications to embedded devices with analog inputs and outputs. The assets in Table 3 that could be susceptible to cyber threat actors include control servers, data historians, engineering workstations, field controllers, human-machine interfaces, input/output servers, and SISs/protection relays. MITRE's ICS-specific ATT&CK framework identifies 81 attack techniques that adversaries use against ICS assets. These attack techniques were evaluated for the types of threats vectors that are most likely to occur on MRE system assets.

The MITRE Common Attack Pattern Enumeration and Classification method was considered to understand how an adversary operates during an attack [20]. The method provides information on different types of patterns of attacks and known weaknesses. This method was used to understand the hierarchy of attack patterns for different domains (e.g. software, hardware, communications, supply chain, social engineering, and physical security).

Based on a review of MRE system assets, threat vectors were identified and analyzed further. Examples of types of cyber threats that could affect 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.), known vulnerabilities, and disaster related threats (i.e., shipwrecks or tsunamis). Appendix D identifies the potential threats that were identified as most likely types of vulnerabilities for MRE systems and assets. The cyber threats listed in Appendix D should not be considered comprehensive as they are only intended to represent the current main threats to similar ICS assets. To address any design diversity of MRE systems, a discussion of each of the MRE architectures with subject matter experts and threat modeling for each design could be conducted to address specific threats and vulnerabilities for MRE systems. A supplemental MRE System Cybersecurity Guidance document will provide security controls that can be tailored by the owner and operator prior to and during deployment.

4.2.3 Cybersecurity Risk Analysis

Performing a cybersecurity risk analysis enables owners and operators to understand the cybersecurity risks to their MRE system (i.e., assets, data, operations, etc.) and its end user (i.e., organization, mission, capabilities, etc.) to implement security controls commensurate with their risk tolerance. The cybersecurity risk of an MRE system is based on the likelihood of occurrence of a cyber threat and the consequences to the MRE system and end user if a cyberattack successfully occurs. Therefore, owners/operators of MRE systems need to determine the risks associated with the operation of their specific system. The following

subsections describe the approach to determine cybersecurity risk by performing a vulnerability assessment of the MRE system and assessing the consequences of a cyberattack.

4.2.3.1 Vulnerability Assessment

MRE system owners and operators would initially perform a vulnerability assessment to evaluate the likelihood of occurrence of a threat that can breach security of the MRE system. A qualitative approach was used to qualitatively categorize the cyber vulnerability of the MRE system (LOW, MODERATE or HIGH). The vulnerability assessment took into consideration the assets of the MRE system, susceptibility to a cyberattack (i.e., protection of assets), geography (i.e., deep ocean, surface of ocean, etc.), accessibility to the MRE system and proximity from external sources, and interconnections with other external networks or organizations. To determine the vulnerability categorization of an MRE system and its operation, the following seven metrics are assessed:

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 locations and are 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 (greater than once a week) is graded HIGH vulnerability.
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 systems 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, fence, or container) or if the enclosures are not locked and/or can be accessed by anyone are graded HIGH because these assets be subject to 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 (e.g., 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. If it is not managed at all, then the MRE system 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.

Table 4 summarizes the metrics used to qualitatively assess the vulnerability of an MRE system and the criterion for determining the vulnerability categorization (LOW, MODERATE, or HIGH). A qualitative score of 1, 2, and 3 is used for low, moderate, and high, respectively. In some cases, the metric may not be applicable based on how the organization answers the first metric, so an "N/A" would be graded as 0, Each factor has the same weight, so the average score is calculated over the six factors that contribute to the likelihood of occurrence of a cyber threat exploiting a MRE vulnerability.

Table 4. Metrics that Influence the Vulnerability Assessment

Threat Metrics	MRE System Vulnerability Categorization		
	LOW	MODERATE	HIGH
1. IT/OT Assets and Network Architecture	No IT/OT assets.	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. Geographical Accessibility	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.
5. Access/User Controls	Identification and authentication of users is managed (e.g., least privilege established, role-based, multifactor authentication).	Identification and authentication of users is 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.

Threat Metrics	MRE System Vulnerability Categorization		
	LOW	MODERATE	HIGH
7. Security Controls on Software or Hardware	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).

4.2.3.2 Evaluation of Consequences of a Cyberattack

The impact of a cyberattack of an MRE system can result in both physical and digital effects. As such, a risk assessment also evaluates the potential consequences and impact that a cyberattack would have on the MRE system owner's/operator's mission. The consequences or impact would vary depending on the assets and networks affected by the cyberattack, the extent of infiltration to the networks and control systems, types of information or data affected, and many other factors. Common impacts of a cyberattack include theft of information/data, disruption to operations, threats to human safety, damage to reputation from customers/stakeholders, financial losses due to recovery from the incident, and fines and penalties to regulators. The owner/operator and end user determine the consequences based on the impact to its business and mission objectives.

NIST SP 800-82, *Guide to Industrial Control Systems (ICS) Security*, identifies recommended security controls to mitigate the consequences on safety, physical impact on the ICS and the physical environment, and consequences to non-digital control components within an ICS [22]. The physical consequences to the MRE system were evaluated for the end user's mission (i.e., loss of power from the MRE system). The consequence to human safety considers whether injury, disease, or death is possible from a malfunction of the MRE system. Environmental consequences were also addressed because of the geographical location of these MRE systems by considering if the deployment of the MRE system may have short- and/or long-term impacts on the marine environment, including animals, habitats, and ecosystems.

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 **Error! Reference source not found.**. 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 asset. 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 affects 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 ICS and supporting infrastructure or 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) are 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) are 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 results in loss of data or information (MRE system or end-user data) are also factored into the risk assessment. If the loss of data generated, stored, and transmitted in an MRE system does not affect the mission or end use (i.e., loss of confidentiality, integrity, and availability), 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 major.
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.

Table 5 includes factors that are addressed in the assessment of consequences. The assessment involves a qualitative approach to determine whether the consequences of a cyberattack are low, moderate, or high. For each consequence factor, a graded approach is used to determine the consequence of a cyberattack to allow the MRE system owner and operator flexibility determining the cybersecurity risk.

Table 5. Consequences Assessment of a Cyberattack

Consequence Factors	LOW Score= 1	MODERATE Score = 2	HIGH 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 only minor damage (i.e., redundant controls available, non-digital mechanisms provided such as audio alarms, manual valves to protect the physical boundary).	Significant physical damage to assets, supporting infrastructure, and human safety (e.g., manipulation of controls).	Major physical damage to assets and supporting infrastructure and impact to environment (e.g., damage to 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.

The MRE system operator and owner assess the consequences of a cyberattack by rating each of the consequence factors.

4.2.4 Risk Categorization and Prioritization

The MRE system risk model determines the risk levels based on likelihood of vulnerability and the consequence to an MRE system. The risk is identified in three progressive levels, with Risk Level 1 being the lowest and Risk Level 3 being the highest cybersecurity risk as shown in Table 6. The risk level is a graded approach to manage cybersecurity vulnerabilities and is based on a qualitative assessment of the likelihood of cybersecurity threats and the impact a cybersecurity attack would have on the MRE system and end use. The graded approach provides MRE system owners flexibility to ascertain the number of security controls to prevent, and mitigate a potential cyberattack. The MRE system owner/operator prioritizes risk based on the cost to implement security controls versus the value of the assets.

Table 6. MRE System Cybersecurity Risk Ranking Chart

Vulnerability	Consequences of Cyberattack		
	LOW = 1	MODERATE = 2	HIGH =3
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. A description of each risk 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).

- **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.

- **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.

The supplemental report for Focus 2, PNNL-30256, *Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems* [27], includes the cybersecurity best practices commensurate with the risk level. The RMF for the MRE industry is a risk-based approach that energy owners and operators can use to prioritize activities involving cybersecurity risk management.

5.0 Conclusion

Technology innovation and market demand for renewable energy sources are driving the MRE industry to develop market-ready devices to power certain markets within the blue economy (e.g., desalination facilities, ocean observation, underwater vehicle charging, isolated coastal communities). The advanced IT/OT used in MRE system designs creates new targets for cyber threat actors with malicious intent to gain unauthorized access to data or disrupt operation of the energy-generating device.

This report described a framework to perform a cybersecurity risk assessment of an MRE system and its end use. The framework includes an evaluation of the cybersecurity vulnerability and consequences. The cybersecurity vulnerabilities are dependent on the IT/OT assets and configuration, which will drive innovation in MRE IT/OT systems, further the development of commercial MRE technologies, and ultimately contribute to the delivery of cost-efficient methods for installation, grid integration, operations, monitoring, maintenance, and decommissioning of MRE technologies. Additionally, minimizing cybersecurity risks can increase investor and stakeholder confidence and help decrease project insurance costs.

The framework includes a risk model that identifies three risk levels (Low, Moderate or High) to categorize the MRE system and its end use. The risk levels reflect a graded approach to provide MRE system owners flexibility to ascertain the number of security controls to implement to prevent and mitigate a potential cyberattack. An accompanying guidance document PNNL-30256, *Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems*, identifies the security measures that can be implemented commensurate with the risk level.

6.0 References

[1] EERE. ND. “Marine and Hydrokinetic Resource Assessment and Characterization.” Energy Efficiency & Renewable Energy, Water Power Technologies Office, U.S. Department of Energy. Accessed on March 9, 2020 at https://www.energy.gov/eere/water/marine-and-hydrokinetic-resource-assessment-and-characterization.

[2] Bhattacharya, S., Preziuso, D.C., Alam, M.E., O’Neil, R.S., and Bhatnagar, D. 2019. 2019. *Understanding the Grid Value Proposition of Marine Energy: An Analytical Approach*, PNNL-28839. Pacific Northwest National Laboratory, Richland, WA.

[3] LiVecchi, A., Copping, A., Jenne, D., Gorton, A., Preus, R., Gill, G., Robichaud, R., Green, R., Geerlofs, S., Gore, S., Hume, D., McShane, W., Schmaus, C., and Spence, H. 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.

[4] Economist Intelligent Unit. 2015. “The Blue Economy: Growth, Opportunity and a Sustainable Ocean Economy.” *The Economist*. Retrieved March 19, 2020 at https://www.eiuperspectives.economist.com/sustainability/blue-economy/white-paper/blue-economy.

[5] 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

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

[7] 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.

[8] 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

[9] Drew B., Plummer, A.R., and Sahinkaya, M.N. 2016. “A Review of Wave Energy Converter Technology.” In *Proceedings of the Institution of Mechanical Engineers, Part A: Journal of Power and Energy*. Vol 223. Accessed March 19, 2020 at https://journals.sagepub.com/doi/abs/10.1243/09576509JPE782

[10] Roberts A., Thomas, B., Sewell P., Khan Z., Balmain, S., and Gillman, J. 2016. “Current Tidal Power Technologies and Their Suitability for Applications in Coastal and Marine Areas.” *Journal of Ocean Engineering and Marine Energy*, 2:227–245. DOI 10.1007/s40722-016-0044-

8. Accessed March 19, 2020 at https://link.springer.com/content/pdf/10.1007%2Fs40722-016-0044-8.pdf.

[11] Neary, M., Previsic, M., Jepsen, R.A., Lawson, M.J., Yu, Y.-H., Copping, A.E., Fontaine, A.A., Hallett, K.C., and Murray, D.K. 2014. *Methodology for Design and Economic Analysis of Marine Energy Conversion (MEC) Technologies*, No. SAND2014-3561C. Sandia National Laboratories, Albuquerque, NM.

[12] CISA. 2019. *MAR-17-352-01 HatMan-Safety System Targeted Malware (Update B)*, Malware Analysis Report. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security.

[13] Ashford, W. 2019. "Cyber Attacks Targeting Industrial Control Systems on the Rise." *Computer Weekly*, 27 March 2019. Accessed March 19, 2020 at https://www.computerweekly.com/news/252460353/Cyber-attacks-targeting-industrial-control-systems-on-the-rise.

[14] CISA. 2017. *State Cybersecurity Governance Case Studies*. Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security. Accessed March 19, 2020 at https://www.cisa.gov/sites/default/files/publications/Cross_Site_Report_and_Case_Studies_508.pdf

[15] DoD. 2014. "Cybersecurity," DoDI 8500.01, U.S. Department of Defense Instruction, March 14, 2014.

[16] DoD. 2016. "Risk Management Framework (RMF) for DoD Information Technology," DODI 8510.01, Change 1, Effective May 24, 2016. U.S. Department of Defense Instruction.

[17] DHS. 2015. *Department of Homeland Cybersecurity and Infrastructure Security Agency Industrial Control System Cyber Emergency Response Team Reports*. Accessed March 19, 2020 at https://www.us-cert.gov/sites/default/files/Annual_Reports/FY2015_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

[18] Dragos. 2019. *Industrial Control System (ICS) Year in Review: The ICS Landscape and Threat Activity Groups*. Accessed on May 31, 2020 at https://dragos.com/resource/dragos-2019-ics-year-in-review-the-ics-threat-landscape-and-activity-groups/

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

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

[21] 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

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

[23] MITRE. ND. Enterprise Matrix. Accessed March 19, 2020 at https://attack.mitre.org/matrices/enterprise/

[24] Dragos. ND. “North American Electric Cyber Threat Perspective.” Accessed March 19, 2020 at https://dragos.com/resource/north-american-electric-cyber-threat-perspective/

[25] DoD. 2014. “Cybersecurity,” DoDI 8500.01, U.S. Department of Defense Instruction, March 14, 2014.

[26] DoD. 2016. “Risk Management Framework (RMF) for DoD Information Technology,” DODI 8510.01, Change 1, Effective May 24, 2016. U.S. Department of Defense Instruction.

[27] PNNL. 2020. *Cybersecurity Best Practice Guidance for Marine Renewable Energy Systems*, PNNL-30256, Pacific Northwest National Laboratory Report. Richland, WA.

[28] Jang-Jaccard, J. and Nepal, Surya. 2014. “A Survey of Emerging Threats in Cybersecurity.” *Journal of Computer and System Sciences*. Volume 80 (2014) pages 973-993.

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

[30] 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.

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

[32] Yu, Y.H., D.S. Jenne, R. Thresher, A. Copping, S. Geerlofs, and L.A. Hanna. 2015. *Reference Model 5 (RM5): Oscillating Surge Wave Energy Converter*, National Renewable Energy Laboratory, Golden, CO.

[33] Labonte, A. 2015., *River Turbine Provides Clean Energy to Remote Alaskan Village,* Department of Energy Office of Energy Efficiency and Renewable Energy article. Accessed on September 29, 2020 at https://www.energy.gov/eere/articles/river-turbine-provides-clean-energy-remote-alaskan-village

[34] Schreiber, M. 2020, *How remote Arctic communities can tap into river power.* Arctic Today, September 3, 2020. Accessed on September 29, 2020 at https://www.arctictoday.com/how-remote-arctic-communities-can-tap-into-river-power/

Appendix A – Definition

Asset	Hardware, software, computer networks, communication methods, applications, and other operational and information technology equipment that would manage data (i.e., collected, used, developed, 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
Developer	Organizations or manufacturers responsible for the MRE system design
End User/Market	The intended client or organization that depends on the electricity generated from the marine renewable energy device
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 an 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 an 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 that can 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 is executing a threat
Vulnerability	Weakness or gap in the protection/security of the marine renewable energy system

Appendix B – Example Marine Renewable Energy System Architectures

Figures B.1 and B.2 showcase an example network architecture for two different MRE system designs. These examples are based on information received in the Requests for Information and directly correspond with current systems developed by real-world developers. These network architectures provide more specific insight into possible threats and threat vectors that MRE experience.

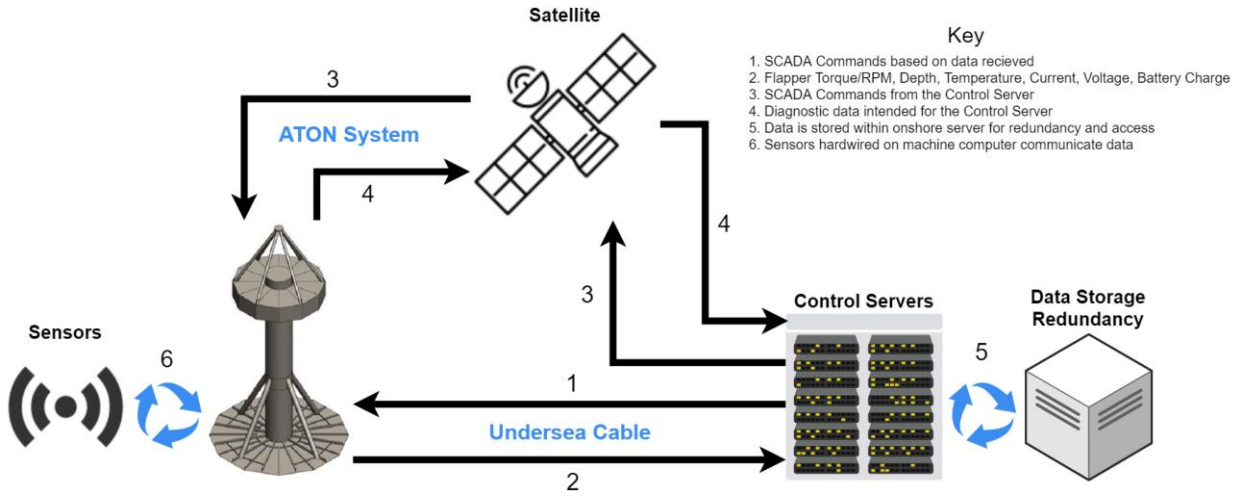


Figure B.1. Example Architecture of a Wave Point Absorber Intended for Large-Scale Grid Power

Figure B.1 details an in-production MRE system that powers the grid through a Wave Point Absorber design. This design connects to a control server onshore via undersea cable, where data from the sensors is offloaded for data redundancy and processing. The system has additional redundancy as the buoy system communicates to a satellite and then back to the onshore control servers.

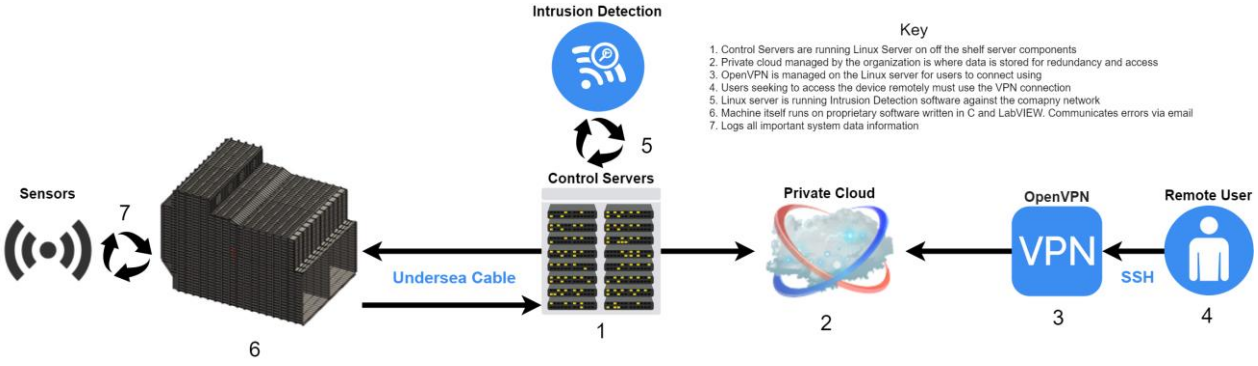


Figure B.2. Example Architecture of an Oscillating Water Column Intended for Large-Scale Grid Power

Figure B.2 details an MRE system that is being designed to power the grid. This system collects information from onboard sensors attached to the MRE device, and then sends the information via undersea cable to onshore control servers. The servers are running a version of Linux and

have intrusion detection software monitoring the network connection. From there, the information is sent to a private cloud, where the information can be accessed by remote users using a virtual private network into the company's network. Table B.1 summarizes the components that could potentially become threat vectors for adversaries.

Table B.1. List of MRE System Assets

Component	Description
Supervisory Control and Data Acquisition System	A control system architecture comprising computers, networked data communications, and graphical user interfaces for high-level process supervisory management.
Wireless Networking	Wireless data communication between network nodes, typically, via several radiofrequency protocols such as 802.11.
Wide Area Network	Network that exists over a large-scale geographical area and connects different smaller networks, including local area networks, and is also used to describe the internet as a whole, including the architecture in place to transverse every publicly facing server.
Local Area Network	Network that spans a relatively small area, like a single room, building, or group of buildings and is also used to describe a local interconnected network that does not directly interface with the wide area network. Typically controlled via routers and switches.
Satellite Transponder	Responsible for managing wireless data communication via satellite.
Cell Tower Transponder	Responsible for managing wireless data communication via cell tower.
Wired Networking	Wired data communication between network nodes, typically via Ethernet or fiber-optic cable.
Networking	Communication between nodes. Can be through a variety of media, both wireless and wired.
Real-Time Operating System	An operating system intended to serve real-time applications that process data as it comes in, typically without buffer delays.
Wireless Access Point	An access point used to connect to a wireless network.
Industrial Control System	A computer system that includes the devices, systems, networks, and controls used to operate and/or automate industrial processes. Typically encompasses devices such as sensors and actuators.
Programmable Logic Controller	An industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices.
Internet of Things	Devices that fall within the category of internet of things. This includes small, simple devices that historically were not directly connected to a network such as a sensor.
Cloud	Generally used to describe a cluster of dedicated storage and computing servers that are centralized and accessible from the wide area network. Typically owned and managed by platform-as-a-service providers.
Private Cloud	See Cloud. Owned and managed by a company for only dedicated internal, proprietary use, rather than by a platform-as-a-service provider.

Component	Description
Virtual Private Network	Extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
Sensor	A device that detects or measures a physical property and records and indicates or otherwise responds to what it detects.
Actuator	A component of a machine that is responsible for moving and controlling a mechanism or system.
Remote Desktop Protocol	A proprietary protocol developed by Microsoft that provides a graphical interface for users to connect to another computer over a network connection.
Secure Shell	A cryptographic network protocol for operating network services securely over an unsecured network. Typical applications include remote command-line, log-in, and remote command execution.
Microprocessor	A computer processor that incorporates the functions of a central processing unit on a single integrated circuit.
Random Access Memory	A form of computer memory that can be read and changed in any order, typically used to store working data and machine code.
Central Processing Unit	Electronic circuitry within a computer that executes instructions that make up a computer program. The central processing unit performs basic arithmetic, logic, controlling, and input/output operations specified by the instructions.
Removable Media	A form of computer storage that is designed to be inserted and removed from a system.
Physical Digital Interfaces	Physical ports that allow digital components to interact with a system or network such as an Ethernet port or Universal Serial Bus port.

Appendix C – Request for Information

Request for Information

Cybersecurity for Marine Renewable Energy Systems

Desired completion date: February 28, 2020

Introduction

On behalf of the U.S. Department of Energy, Pacific Northwest National Laboratory (PNNL) is leading an effort to develop cybersecurity guidance to protect the confidentiality, integrity and availability of marine renewable energy (MRE) systems against potential cyber threats. PNNL is distributing this Request for Information (RFI) to MRE developers to solicit relevant information on MRE designs, applications, and system/network integration mechanisms, which will be used to identify potential cybersecurity threats and consequences to the system design and implementation.

All responses to this RFI and any subsequent discussions with PNNL related to this scope will be used solely to inform the development of cybersecurity guidance and will be kept private.

Affiliation and Contact Information

Name: _____

Affiliation: _____

Contact Information: _____

Technology Design, Application, and Market

Q1. Please select your technology design from the list below and describe its design and configuration.

☐Tidal current turbine ☐River current turbine ☐Wave point absorber
☐Ocean current turbine ☐Oscillating surge flap ☐Oscillating water column
☐Other

Response…

Q2. What is the intended application for this design and the expected end use/market (e.g., grid connection, powering underwater vehicles/buoys, etc.)?

Response…

System and Network Integration

Q3. How will this device communicate with other systems and networks (e.g., wired, wireless, cellular, satellite, Bluetooth, etc.)?

Response…

Q4. What software or firmware is involved in the system design, configuration, and/or development? Are there any on-board or integrated troubleshooting capabilities (i.e. self-diagnostics or system error reports)?

Response…

Q5. Is the platform actively monitored for power generation and/or state of health? If so, describe the monitoring, who is monitoring performance, what performance metrics are monitored, and how does monitoring occur (i.e. specialized software, etc.)?

Response…

Q6. What type of data is generated in this system?

Response…

Q7. How is data managed in your system [e.g., supervisory control and data acquisition (SCADA) systems, programmable logic controllers, hard drives, motherboards, memory capabilities (e.g., random access memory/read-only memory), or other computing components on board the deployed system]?

Response…

Q7. How is data stored, processed and transmitted for this system (e.g., cloud, real-time data transmission, remote server, etc.)?

Response…

Q8. What physical and/or network access mechanisms (including remote access) are incorporated in the system design?

Response…

Q9. Once connected to the system, how are access, accounts and sessions managed (i.e., login/password or other credentials required, multifactor authentications, etc.)?

Response…

Cybersecurity Considerations

Q10. What cybersecurity best practices does your technology implement to protect from potential cyber threats (e.g., virus protection, malware detection, etc.)?

Response…

Q11. What cybersecurity policies, regulatory authorities, requirements, and/or standards apply to your MRE system?

Response…

PNNL Point of Contact:
Fleur de Peralta, P.E. – fleurdeliza.deperalta@pnnl.gov; Office: (509) 375-3323

Appendix D – Potential Threats to MRE Systems

The potential cyber threats analyzed were based on the context of six various MRE system designs and information obtained from available open sources from the public and private industrial control system cybersecurity leaders, such as ICS-CERT, Dragos [24], and MITRE [19,23].

Table D.1. MRE System Threats

MRE Threat Types and Subcategories	Description
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.
Data Theft	An adversary steals MRE development/operational data.
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.
Denial of Service	An attacker attempts to prevent normal MRE staff and/or customer activity.
Identity Theft	An adversary steals personal identification information for unauthorized use.
Malware	An adversary installs or adds malicious logic (also known as malware) into a seemingly benign MRE component of a fielded system.
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.
Social Engineering (Phishing)	An attacker masquerades as a legitimate entity with which the MRE staff might do business to prompt the user to reveal some confidential information (very frequently authentication credentials).
Supply Chain	An attacker disrupts the MRE supply chain life cycle by manipulating system hardware, software, or services.
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.
Targeted Malware	An adversary develops MRE-targeted malware that takes advantage of a known vulnerability in an MRE system.
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.
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.
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.

MRE Threat Types and Subcategories	Description
Vulnerability Scanning	An attacker engages in scanning activity to find vulnerable MRE software versions or types, such as operating system versions or network services.
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 passed on to the other component as if it were never observed.
Accidental Damage	
Incorrect OT System Administration	Erroneous actions taken by MRE operators/engineers, IT, and/or vendors when executing their everyday responsibilities.
Misconfigured IT-Managed Security Services	Dependent IT security managed services not configured correctly to monitor MRE system.
Data Loss	The exposure of MRE proprietary or business-sensitive information through either data theft or data leakage.
Physical Attacks	
Sabotage	An adversary deliberately manipulates the MRE safety system operation such that it either 1) does not operate when needed or 2) performs incorrect control actions that damage the MRE system.
Vandalism	An adversary causes physical damage to an MRE asset or other resource.
Theft	An adversary steals a physical MRE system asset or other resource.
Unauthorized Access	An adversary gains physical access to an MRE asset or other resource without permission.
Terrorism	An adversary uses traditional attack methods (e.g., bomb) to destroy, incapacitate, or exploit the MRE system for religious, political, or ideological reasons.
Hacktivism	An adversary uses technology to destroy, incapacitate, or exploit the MRE system to promote a political or social agenda.
Organized Crime	An adversary (e.g., pirates) attacks the MRE system for monetary gain.
Infrastructural/Component Failures and Malfunctions	
Failures or Malfunctions of MRE System or Devices	A failure or malfunction of the MRE system or resource.
Known Vulnerabilities	An MRE system asset with known security weaknesses that could be exploited by an adversary.
Improper Network Architecture	An adversary engages undetected in lateral movement through the network (e.g., nodes, hosts, devices, and routes).
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).
Disasters	
Environmental	A catastrophic human incident causing unfavorable environmental conditions, such as a shipwreck.
Natural	A major adverse event resulting from natural processes of the earth, such as a cyclonic storm, tsunami, heavy winds.

Pacific Northwest National Laboratory

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

www.pnnl.gov