9110-04-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Parts 101 and 160

[Docket No. USCG-2022-0802]

RIN 1625-AC77

Cybersecurity in the Marine Transportation System

AGENCY: Coast Guard, Department of Homeland Security (DHS).

ACTION: Notice of proposed rulemaking.

SUMMARY: The Coast Guard proposes to update its maritime security regulations by adding regulations specifically focused on establishing minimum cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf facilities, and U.S. facilities subject to the Maritime Transportation Security Act of 2002 regulations. This proposed rule would help to address current and emerging cybersecurity threats in the marine transportation system. We seek your comments on this proposed rule and whether we should: use and define the term *reportable cyber incident* to limit cyber incidents that trigger reporting requirements, use alternative methods of reporting such incidents, and amend the definition of *hazardous condition.*

DATES: Comments and related material must be received by the Coast Guard on or before [INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments identified by docket number USCG-2022-0802 using the Federal Decision-Making Portal at www.regulations.gov. See the "Public Participation and Request for Comments" portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments. You may also find this notice of proposed rulemaking, with its 100-word-or-less summary, in this

same docket at www.regulations.gov.

Collection of information. Submit comments on the collection of information discussed in section VI.D of this preamble both to the Coast Guard's online docket and to the Office of Information and Regulatory Affairs (OIRA) in the White House Office of Management and Budget (OMB) using their website, www.reginfo.gov/public/do/PRAMain. Comments sent to OIRA on the collection of information must reach OIRA on or before the comment due date listed on their website.

FOR FURTHER INFORMATION CONTACT: For information about this document, email MTSCyberRule@uscg.mil or call: Commander Brandon Link, Office of Port and Facility Compliance, 202-372-1107, or Commander Frank Strom, Office of Design and Engineering Standards, 202-372-1375.

SUPPLEMENTARY INFORMATION:

Table of Contents for Preamble

I. Public Participation and Request for Comments

The Coast Guard views public participation as essential to effective rulemaking and will consider all comments and material received during the comment period. Your comment can help shape the outcome of this rulemaking. If you submit a comment, please include the docket number for this rulemaking, indicate the specific section of this document to which each comment applies, and provide a reason for each suggestion or recommendation.

Submitting comments. We encourage you to submit comments through the Federal Decision-Making Portal at www.regulations.gov. To do so, go to www.regulations.gov, type USCG-2022-0802 in the search box and click "Search." Next, look for this document in the **Search Results** column, and click on it. Then click on the **Comment** option. If you cannot submit your material by using www.regulations.gov, call or email the persons in the **FOR FURTHER INFORMATION CONTACT** section of this proposed rule for alternate instructions.

Viewing material in docket. To view documents mentioned in this proposed rule as being available in the docket, find the docket as described in the previous paragraph, and then select "Supporting & Related Material" in the Document Type column. Public comments will also be placed in our online docket and can be viewed by following instructions on the www.regulations.gov Frequently Asked Questions (FAQ) webpage. That FAQ page also explains how to subscribe for email alerts that will notify you when comments are posted or if a final rule is published. We review all comments received, but we will only post comments that address the topic of the proposed rule. We may choose not to post off-topic, inappropriate, or duplicate comments that we receive.

Personal information. We accept anonymous comments. Comments we post to www.regulations.gov will include any personal information you have provided. For more about privacy and submissions to the docket in response to this document, see the

Department of Homeland Security's eRulemaking System of Records notice (85 FR 14226, March 11, 2020).

Public meeting. We do not plan to hold a public meeting, but we will consider doing so if we determine from public comments that a meeting would be helpful. We would issue a separate **Federal Register** notice to announce the date, time, and location of such a meeting.

II. Abbreviations

AMSC	Area Maritime Security Committees
BLS	Bureau of Labor Statistics
CEA	Council of Economic Advisors
CFR	Code of Federal Regulations
CGCSO	Coast Guard Cyber Strategic Outlook
CG-CVC	Coast Guard Office of Commercial Vessel Compliance
CGCYBER	U.S. Coast Guard Cyber Command
CG-ENG	Coast Guard Office of Design and Engineering Standards
CG-FAC	Coast Guard Office of Port and Facility Compliance
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
COTP	Captain of the Port
CPG	Cybersecurity Performance Goal
CRM	Cyber risk management
CSF	Cybersecurity framework
CSRC	Computer Secure Resource Center
CySO	Cybersecurity officer
DHS	Department of Homeland Security
FR	**Federal Register**
FSA	Facility security assessment
FSP	Facility security plan
HMI	Human-machine interface
ICR	Information collection request
IEc	Industrial Economics, Incorporated
IMO	International Maritime Organization
IP	Internet protocol
IRFA	Initial Regulatory Flexibility analysis
ISM	International Safety Management
IT	Information technology
KEV	Known exploited vulnerability
MCAAG	Maritime Cybersecurity Assessment and Annex Guide
MISLE	Marine Information for Safety and Law Enforcement
MODU	Mobile offshore drilling unit
MSC	Marine Safety Center
MSC-FAL	International Maritime Organization's Marine Safety Committee and Facilitation Committee
MTS	Marine transportation system
MTSA	Maritime Transportation Security Act of 2002

NAICS	North American Industry Classification System
NIST	National Institute of Standards and Technology
NMSAC	National Maritime Security Advisory Committee
NPRM	Notice of proposed rulemaking
NRC	National Response Center
NVIC	Navigation and Vessel Inspection Circular
OCMI	Officer in Charge, Marine Inspection
OCS	Outer continental shelf
OEWS	Occupational Employment and Wage Statistics
OMB	Office of Management and Budget
OSV	Offshore supply vessel
OT	Operational technology
PII	Personally identifiable information
QCEW	Quarterly Census of Employment and Wages
RIA	Regulatory impact analysis
§	Section
SBA	Small Business Administration
SME	Subject matter expert
SMS	Safety management system
TSI	Transportation security incident
U.S.C.	United States Code
VSA	Vessel security assessment
VSP	Vessel security plan

III. Basis and Purpose

A. The Problem We Seek to Address

The maritime industry is undergoing a significant transformation that involves increased use of cyber-connected systems. While these systems improve commercial vessel and port facility operations, they also bring a new set of challenges affecting design, operations, safety, security, training, and the workforce.

Every day, malicious actors (including, but not limited to, individuals, groups, and adversary nations posing a threat) attempt unauthorized access to control system devices or networks using various communication channels. An example of a successful attempt occurred in May 2021, when the Colonial Pipeline Company suffered a cyber-attack that disrupted the supply of fuel to the east coast of the United States. These cybersecurity threats require the maritime community to effectively manage constantly changing risks to create a safer cyber environment.

The purpose of this notice of proposed rulemaking (NPRM) is to safeguard the marine transportation system (MTS) against current and emerging threats associated with cybersecurity by adding minimum cybersecurity requirements to part 101 of title 33 of the Code of Federal Regulations (CFR) to help detect, respond to, and recover from cybersecurity risks that may cause transportation security incidents (TSIs). This proposed rule would help address current and emerging cybersecurity threats to maritime security in the MTS.

Cybersecurity risks result from vulnerabilities in the operation of vital systems, which increase the likelihood of cyber-attacks on facilities, Outer Continental Shelf (OCS) facilities, and vessels. Cyber-related risks to the maritime domain are threats to the critical infrastructure that citizens and companies depend on to fulfill their daily needs. Additionally, the proposed rule is necessary because it would create a regulatory environment for cybersecurity in the maritime domain to assist facilities, OCS facilities, and vessel firms that may not have taken cybersecurity measures on their own, for various reasons. In a 2018 report by the Council of Economic Advisors (CEA), the CEA stated "[a] firm with weak cybersecurity imposes negative externalities on its customers, employees, and other firms, tied to it through partnerships and supply chain relations. In the presence of externalities, firms would rationally underinvest in cybersecurity relative to the socially optimal level. Therefore, it often falls to regulators to devise a series of penalties and incentives to increase the level of investment to the desired level."[1]

In the report, the CEA also emphasized that "[c]ontinued cooperation between the public and private sectors is the key to effectively managing cybersecurity risks. . . . The government is likewise important in incentivizing cyber protection—for example, by disseminating new cybersecurity standards, sharing best practices, conducting basic

[1] Economic Report of the President Together with the Annual Report of the Council of Economic Advisers (Feb. 2018), https://www.govinfo.gov/content/pkg/ERP-2018/pdf/ERP-2018.pdf (accessed Dec. 15, 2023). Page 323-324.

research on cybersecurity, protecting critical infrastructures, preparing future employees for the cybersecurity workforce, and enforcing the rule of law in cyberspace."[2]

Furthermore, the CEA acknowledged that "[f]irms and private individuals are often outmatched by sophisticated cyber adversaries. Even large firms with substantial resources committed to cybersecurity may be helpless against attacks by sophisticated nation-states."[3] As an example, the CEA stated, "firms that own critical infrastructure assets, such as parts of the nation's power grid, may generate pervasive negative spillover effects for the wider economy."[4]

Lastly, the CEA stated another problem that exists in the marketplace is, "firms' reluctance to share information on cyber threats and exposures", which "impairs effective cybersecurity."[5] The CEA further stated that "firms remain reluctant to increase their exposure to legal and public affairs risks. The lack of information on cyberattacks and data breaches suffered by other firms may cause less sophisticated small firms to conclude that cybersecurity risk is not a pressing problem. . . . [T]he lack of data may be stymying the ability of law enforcement and other actors to respond quickly and effectively and may be slowing the development of the cyber insurance market."[6]

This proposed rule would apply to the owners and operators of U.S.-flagged vessels subject to 33 CFR part 104 (Maritime Security: Vessels), facilities subject to 33 CFR part 105 (Maritime Security: Facilities), and OCS facilities subject to 33 CFR part 106 (Marine Security: Outer Continental Shelf (OCS) Facilities). The proposed requirements include account security measures, device security measures, data security measures, governance and training, risk management, supply chain management, resilience, network segmentation, reporting, and physical security.

---

[2] Id. at 324-325.
[3] Id. at 326.
[4] Id. at 326.
[5] Id. at 326.
[6] Id. at 326.

This NPRM also seeks public comments specifically on defining a *reportable cyber incident* in 33 CFR 101.615 and using that term to limit reporting requirements; whether certain reports required under proposed §§ 101.620 and 101.650 should be sent to the Cybersecurity and Infrastructure Security Agency (CISA); and whether to amend the definition of *hazardous condition* in 33 CFR part 160. We will consider comments on these three issues in deciding whether to amend the regulatory text we have proposed.

The Coast Guard welcomes comments on all aspects of this rulemaking, including the proposed changes to definitions and the assumptions and estimates in section VI.A., *Regulatory Planning and Review*. Section VI.A. of this preamble addresses, for instance, developing a Cybersecurity Plan and cybersecurity drill components, the affected population, device security measures, supply chain management, network segmentation, physical security, implementing and maintaining multifactor authentication, and owners and operators' existing practices on the proposed cybersecurity measures.

B. Recent Legislation, Regulations, and Policy

In the Maritime Transportation Security Act of 2002 (MTSA),[7] Congress provided a framework for the Secretary of Homeland Security ("Secretary"), acting through the Coast Guard,[8] and maritime industry to identify, assess, and prevent TSIs in the MTS. MTSA vested the Secretary with authorities for broad security assessment, planning, prevention, and response activities to address TSIs, including the authority to require and set standards for Facility Security Plans (FSPs), OCS FSPs, and Vessel Security Plans (VSPs), to review and approve such plans, and to conduct inspections and take enforcement actions.[9] The Coast Guard's implementing regulations address a range of considerations to deter TSIs to the maximum extent practicable,[10] and require, among

[7] Pub. L. 107-295, 116 Stat. 2064, November 25, 2002.
[8] The Secretary delegated this authority to the Commandant of the Coast Guard via Department of Homeland Security (DHS) Delegation 00170.1(II)(97)(b), Revision No. 01.3.
[9] *See generally, for example*, 46 U.S.C. 70103.
[10] *See* 46 U.S.C. 70103(c)(1).

other general and specific measures, security assessments and measures related to radio and telecommunication systems, including computer systems and networks.[11]

The Coast Guard has also issued additional guidance and policies to address potential cyber incidents in FSPs, OCS FSPs, and VSPs,[12] including a cybersecurity risk assessment model that was issued in January 2023,[13] and voluntary guidance issued to Area Maritime Security Committees (AMSC) in July 2023.[14] Congress has repeatedly reaffirmed the MTSA framework, including through amendments passed in 2016,[15] 2018,[16] and 2021.[17] In the 2018 amendments, Congress amended MTSA to specifically require VSPs and FSPs to include provisions for detecting, responding to, and recovering from cybersecurity risks that may cause TSIs.[18] The proposed regulatory amendments to 33 CFR part 101 reflect the Coast Guard's view on cybersecurity under MTSA, including, but not limited to, recent amendments to MTSA (such as Title 46 of the United States Code (U.S.C.) Section 70103). The proposed amendments provide more detailed mandatory baseline requirements for U.S.-flagged vessels and U.S. facilities subject to MTSA.

---

[11] *See, for example*, 33 CFR 104.300(d)(11), 104.305(d)(2)(v), 105.300(d)(11), 105.305(c)(1)(v), 106.300(d)(11), 106.305(c)(1)(v), and 106.305(d)(2)(v).

[12] One of the Coast Guard's guidance documents is the Navigation and Vessel Inspection Circular (NVIC) 01-20, *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act Regulated Facilities* (85 FR 16108). This NVIC outlined Coast Guard's view on requirements for FSPs and facility security, including cybersecurity. A similar understanding with regard to VSPs was expressed in the Coast Guard's Office of Commercial Vessel Compliance's (CG-CVC) Vessel CRM Work Instruction CVC-WI-027(2), *Vessel Cyber Risk Management Work Instruction*, October 27, 2020, https://www.dco.uscg.mil/Portals/9/CVC-WI-27%282%29.pdf, accessed July 18, 2023.

[13] *See* Maritime Cybersecurity Assessment and Annex Guide (MCAAG) (January 2023), https://dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment%20%20Annex%20Guide%20(MCAAG)_released%2023JAN2023.pdf, accessed Aug. 4, 2023. The MCAAG was developed in coordination with the National Maritime Security Advisory Committee, AMSCs, and other maritime stakeholders. The guide serves as a resource for baseline cybersecurity assessments and plan development and helps stakeholders address vulnerabilities that could lead to transportation security incidents.

[14] NVIC 09-02, Change 6.

[15] Pub. L. 114-120, 130 Stat. 27, February 8, 2016.

[16] Pub. L. 115-254, 132 Stat. 3186, October 5, 2018.

[17] Pub. L. 116-283, 134 Stat 4754, January 1, 2021.

[18] *See* Pub. L. 115-254, sec. 1805(d)(2) (codified at 46 U.S.C. 70103(c)(3)(C)).

Through three administrations, presidential policy has advanced cybersecurity in the maritime domain. Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity) recognized the Federal Government's efforts to secure our nation's critical infrastructure by working with the owners and operators of U.S. facilities, OCS facilities, and U.S.-flagged vessels to prepare for, prevent, mitigate, and respond to cybersecurity threats.[19]

To defend against malicious cyber-related activities, Executive Order 13694 of April 1, 2015 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities) recognized malicious cyber-related activities as an "extraordinary threat to the national security, foreign policy, and economy of the United States," warranting a national emergency.[20] The National Emergency with Respect to Significant Malicious Cyber-Enabled Activities has been extended as of March 30, 2023.[21]

Executive Order 14028 of May 12, 2021 (Improving the Nation's Cybersecurity) also recognized that "the private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace."[22]

On July 28, 2021, the President issued the "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,"[23] which required the Secretary of Homeland Security to coordinate with the Secretary of Commerce (through the Director of the National Institute of Standards and Technology (NIST)) and

---

[19] 78 FR 11739, February 19, 2013.
[20] 80 FR 18077, April 2, 2015. Executive Order 13694 was later amended by Executive Order 13757 (82 FR 1, January 3, 2017), which outlined additional measures the Federal Government must take to address the national emergency identified in Executive Order 13694.
[21] 88 FR 19209, March 30, 2023.
[22] 86 FR 26633.
[23] The White House, National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/, last accessed on July 24, 2023.

other agencies, as appropriate, to develop baseline Cybersecurity Performance Goals (CPGs). These baseline CPGs would further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety. CISA's release of the CPGs in October 2022 was "intended to help establish a common set of fundamental cybersecurity practices for critical infrastructure, and especially help small- and medium-sized organizations kickstart their cybersecurity efforts."[24] The Coast Guard relied on CISA's CPGs as the benchmark for technical requirements in this proposed rule.

In 2021, the Coast Guard published its Cyber Strategic Outlook (CGCSO) to highlight the importance of managing cybersecurity risks in the MTS.[25] The CGCSO highlighted three lines of effort, or priorities, to improve Coast Guard readiness in cyberspace: (1) Defend and Operate the Coast Guard Enterprise Mission Platform; (2) Protect the MTS; and (3) Operate in and through Cyberspace.[26] As outlined in the CGCSO's second line of effort, "Protect the MTS," the Coast Guard proposes to implement a risk-based regulatory, compliance, and assessment regime. We propose to establish minimum requirements for cybersecurity plans that facilitate the use of international and industry-recognized cybersecurity standards to manage cybersecurity risks by owners and operators of maritime critical infrastructure.[27] Specifically, this

---

[24] CISA, "Cross-Sector Cybersecurity Performance Goals," https://www.cisa.gov/cross-sector-cybersecurity-performance-goals, accessed July 18, 2023.
[25] U.S. Coast Guard, "Cyber Strategic Outlook," August 2021, https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf, accessed July 18, 2023.
[26] These lines of effort evolved from the three "strategic priorities" introduced in the Coast Guard's Cyber Strategy, June 2015. As cyber threats and vulnerabilities evolve, so will the Coast Guard's posture. https://www.dco.uscg.mil/Portals/10/Cyber/Docs/CG_Cyber_Strategy.pdf?ver=nejX4g9gQdBG29cX1HwFdA%3D%3D, accessed July 18, 2023.
[27] The Coast Guard is aware that some entities already follow industry standards related to cybersecurity. The proposed minimum requirements seek to establish a common baseline for all the regulated vessels and facilities that would not be incompatible with such standards, recognizing that in some instances these proposed minimums may increase a requirement, but in other circumstances will already be satisfied. The entity would be able to indicate within their Cyber Plan that they are following a particular standard and highlight how their compliance with that standard satisfies the Coast Guard requirements.

proposed rule would promulgate the Coast Guard's baseline cybersecurity regulations for U.S.-flagged vessels and U.S. facilities (including OCS facilities) subject to MTSA.

As noted, in January 2023, the Coast Guard released the Maritime Cybersecurity Assessment and Annex Guide (MCAAG). The MCAAG was developed through coordination with the National Maritime Security Advisory Committee, Area Maritime Security Committees, and other maritime stakeholders, consistent with the activities described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)). The MCAAG provides more detailed recommendations on implementing existing MTSA regulations as they relate to computer systems and networks. For example, the Coast Guard recommended a Cyber Annex Template for stakeholders to address possible cybersecurity vulnerabilities and risks.

This NPRM is meant to expand and clarify the information required in security plans to remain consistent with 46 U.S.C. 70103(c)(3), including section 70103(c)(3)(C)(v), which requires FSPs, OCS FSPs, and VSPs to include provisions for detecting, responding to, and recovering from cybersecurity risks that may cause TSIs. Some terms we use in the MCAAG, such as *cybersecurity vulnerability*, may have a set proposed definition in this NPRM.

C. Legal Authority to Address This Problem

The Coast Guard is proposing to promulgate these regulations under 43 U.S.C. 1333(d); 46 U.S.C. 3306, 3703, 70102 through 70104, 70124; and the Department of Homeland Security (DHS) Delegation No. 00170, Revision No. 01.3.

Section 4 of the Outer Continental Shelf Lands Act of 1953, codified as amended at 43 U.S.C. 1333(d), authorizes the Secretary to promulgate regulations with respect to lights and other warning devices, safety equipment, and other matters relating to the promotion of safety of life and property on the artificial islands, installations, and other

devices on the OCS. This authority was delegated to the Coast Guard by DHS Delegation No. 00170(II)(90), Revision No. 01.3.

Section 3306 of Title 46 of the United States Code authorizes the Secretary to prescribe necessary regulations for the design, construction, alteration, repair, equipping, manning and operation of vessels and prevention and mitigation of damage to the marine environment, propulsion machinery, auxiliary machinery, boilers, unfired pressure vessels, piping, electric installations, and accommodations for passengers and crew. This authority was delegated to the Coast Guard by DHS Delegation No. 00170(II)(92)(b), Revision No. 01.3.

Section 3703 of Title 46 of the United States Code authorizes the Secretary to prescribe similar regulations relating to tank vessels that carry liquid bulk dangerous cargoes, including the design, construction, alteration, repair, maintenance, operation, equipping, personnel qualification, and manning of the vessels. This authority was delegated to the Coast Guard by DHS Delegation No. 00170(II)(92)(b), Revision No. 01.3.

Sections 70102 through 70104 of Title 46 of the United States Code authorize the Secretary to evaluate for compliance vessel and facility vulnerability assessments, security plans, and response plans. Section 70124 authorizes the Secretary to promulgate regulations to implement Chapter 701, including sections 70102 through 70104, dealing with vulnerability assessments for the security of vessels, facilities, and OCS facilities; VSPs, FSPs, and OCS FSPs; and response plans for vessels, facilities, and OCS facilities. These authorities were delegated to the Coast Guard by DHS Delegation No. 00170(II)(97)(a) through (c), Revision No. 01.3.

IV. Background

A. The Current State of Cybersecurity in the MTS

The maritime industry is relying increasingly on digital solutions for operational optimization, cost savings, safety improvements, and more sustainable business. However, these developments, to a large extent, rely on information technology (IT) systems and operational technology (OT) systems, which increases potential cyber vulnerabilities and risks. Cybersecurity risks result from vulnerabilities in secure and safe operation of vital systems, which increase the likelihood of cyber-attacks on U.S. facilities, OCS facilities, and U.S.-flagged vessels.

Cyber-attacks on public infrastructure have raised awareness of the need to protect systems and equipment that facilitate operations within the MTS because cyber-attacks have the potential to disable the IT and OT onboard U.S.-flagged vessels, U.S. facilities, and OCS facilities. Autonomous vessel technology, automated OT, and remotely operated machines provide further opportunities for cyber-attackers. These systems and equipment are prime targets for cyber-attacks stemming from insider threats, criminal organizations, nation state actors, and others.

Also, the MTS has become increasingly susceptible to cyber-attacks due to the growing integration of digital technologies in their operations. These types of cyber-attacks can range from altering a vessel's navigational systems to disrupting its communication with ports, which can lead to delays, accidents, or even potential groundings that could potentially disrupt vessel movements and shut down port operations, such as loading and unloading cargo. This disruption can also negatively affect the MTS by interrupting the transportation and commerce of goods, raw resources, and passengers, as well as potential military operations when needed.

An attack that compromises navigational or operational systems can pose a serious safety risk. It could result in accidents at sea, potential environmental disasters like oil spills, and loss of life. The maritime industry is not immune to ransomware attacks where cybercriminals are targeting critical systems or data. Given the critical

nature of marine transportation to global trade, continued efforts are being made to improve cybersecurity measures in the sector.

Maritime stakeholders can better detect, respond to, and recover from cybersecurity risks that may cause TSIs by adopting a range of cyber risk management (CRM) measures, as described in this proposed rule. It is important that the Coast Guard work with the maritime community to address both safety and security risks to better facilitate operations and to protect MTS entities from creating hazardous conditions within ports and waterways. Updating regulations to include minimum cybersecurity requirements would strengthen the security posture and increase resilience against cybersecurity threats in the MTS.

In 2017, the International Maritime Organization (IMO) took steps to address cybersecurity risks in the shipping industry by publishing the Marine Safety Committee/Facilitation Committee (MSC-FAL) Circular 3, *Guidelines on Maritime Cyber Risk Management*,[28] and MSC Resolution 428(98).[29] The IMO affirmed that an approved Safety Management System (SMS) should involve CRM to manage cybersecurity risks in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code. An SMS is a structured and documented set of procedures enabling company and vessel personnel to effectively implement safety and environmental protection policies that are specific to that company or vessel.

For applicable U.S.-flagged vessels, this proposed rule would establish a baseline level of protection throughout the MTSA-regulated vessel fleet. As the flag state, the Coast Guard can ensure these proposed cybersecurity regulations are implemented

---

[28] https://www.cdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf, accessed July 18, 2023.

[29] See the IMO resolution on CRM: Resolution MSC.428(98), Annex 10, "Maritime Cyber Risk Management in Safety Management Systems." https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf , accessed July 18, 2023.

appropriately by approving Cybersecurity Plans and conducting routine inspections. This proposed rule would also apply to U.S. facilities regulated by 33 CFR part 105 and OCS facilities regulated by 33 CFR part 106.

B. Current Regulations related to Cybersecurity

The MTSA-implementing regulations in 33 CFR parts 101, 103, 104, 105, and 106 give the Coast Guard the authority to review and approve security assessments and plans that apply broadly to the various security threats facing the maritime industry. Through the Navigation and Vessel Inspection Circular (NVIC) 01-20[30] (85 FR 16108, March 20, 2020), the Coast Guard interpreted 33 CFR parts 105 and 106 as requiring owners and operators of U.S. facilities and OCS facilities to address cybersecurity in their facility security assessments (FSAs) and OCS FSAs, as well as in their FSPs and OCS FSPs, and provided non-binding guidance on how regulated entities could address these issues.

This proposed rule would expand upon the agency's prior actions by establishing minimum performance-based cybersecurity requirements for the MTS within the MTSA regulations. Similar to the existing requirements in 33 CFR parts 104, 105 and 106, the Coast Guard would allow owners and operators the flexibility to determine the best way to implement and comply with these new requirements. The Coast Guard is proposing an implementation period of 12 to 18 months following the effective date of a final rule to allow sufficient time for the owners and operators of applicable U.S.-flagged vessels, U.S. facilities, and OCS facilities to comply with the requirements of this proposed rule.[31]

V. Discussion of Proposed Rule

This NPRM proposes to add minimum cybersecurity requirements to 33 CFR part 101. The Coast Guard invites comment on whether any of the proposed requirements

[30] See footnote 12.
[31] Existing general requirements to address cyber issues in security plans will continue to apply during this rulemaking.

would overlap, conflict, or duplicate existing regulatory requirements from other Federal agencies. The requirements would consist of the following sections:

- 101.600 Purpose
- 101.605 Applicability
- 101.610 Federalism
- 101.615 Definitions
- 101.620 Owner or Operator
- 101.625 Cybersecurity Officer
- 101.630 Cybersecurity Plan
- 101.635 Drills and Exercises
- 101.640 Records and Documentation
- 101.645 Communications
- 101.650 Cybersecurity Measures
- 101.655 Cybersecurity Compliance Dates
- 101.660 Cybersecurity Compliance Documentation
- 101.665 Noncompliance, Waivers, and Equivalents

In addition, the Coast Guard seeks comments on whether, in this rulemaking, we should: define the term *reportable cyber incident* in proposed 33 CFR 101.615 and use that term in the regulatory text to limit cyber incidents that trigger reporting requirements; require certain reports identified in §§ 101.620 and 101.650 to be sent to CISA; and amend the definition of *hazardous condition* in 33 CFR 160.202.

A section-by-section explanation of the proposed additions and changes follows:

Section 101.600—Purpose.

This proposed section states that the purpose of 33 CFR part 101, subpart F, is to set minimum cybersecurity requirements for U.S.-flagged vessels, U.S. facilities, and OCS facilities to safeguard and ensure the security and resilience of the MTS. The

proposed requirements would help safeguard the MTS from the evolving risks of cyber threats and align with the DHS goal of protecting critical U.S. infrastructure.

Section 101.605—Applicability.

This section proposes to make subpart F apply to the owners and operators of the U.S.-flagged vessels listed in 33 CFR 104.105(a), the facilities listed in 33 CFR 105.105(a), and the OCS facilities listed in 33 CFR 106.105(a). A list of the vessels that would be subject to subpart F is as follows:

- U.S. Mobile Offshore Drilling Units (MODUs), cargo vessels, or passenger vessels subject to the International Convention for Safety of Life at Sea, 1974, (SOLAS), Chapter XI-1 or Chapter XI-2;
- Self-propelled U.S. cargo vessels greater than 100 gross register tons subject to 46 CFR chapter I, subchapter I, except commercial fishing vessels inspected under 46 CFR part 105;
- U.S. vessels subject to 46 CFR chapter I, subchapter L;
- U.S. passenger vessels subject to 46 CFR chapter I, subchapter H;
- U.S. passenger vessels certificated to carry more than 150 passengers;
- U.S. passenger vessels carrying more than 12 passengers, including at least 1 passenger-for-hire, that are engaged on an international voyage;
- U.S. barges subject to 46 CFR chapter I, subchapter D or O;
- U.S. barges carrying certain dangerous cargo in bulk or barges that are subject to 46 CFR chapter I, subchapter I, that are engaged on an international voyage;
- U.S. tankships subject to 46 CFR chapter I, subchapter D or O; and
- U.S. towing vessels greater than 8 meters (26 feet) in registered length inspected under 46 CFR subchapter M that are engaged in towing a barge or barges and subject to 33 CFR part 104, except a towing vessel that—

- Temporarily assists another vessel engaged in towing a barge or barges subject to 33 CFR part 104;
- Shifts a barge or barges subject to this part at a facility or within a fleeting facility;
- Assists sections of a tow through a lock; or
- Provides emergency assistance.

This proposed rule would not apply to any foreign-flagged vessels subject to 33 CFR part 104. Cyber regulations for foreign-flagged vessels under domestic law may create unintended consequences with the ongoing and future diplomatic efforts to address maritime cybersecurity in the international arena. The IMO addressed cybersecurity measures for foreign-flagged vessels through MSC-FAL.1/Circ.3 and MSC Resolution 428(98). Therefore, based on IMO guidelines and recommendations, an SMS approved under the ISM Code should address foreign-flagged vessel cybersecurity.

In addition, the Coast Guard verifies how CRM is incorporated into a vessel's SMS via the process described in the October 27, 2020, CVC-WI-027(2), *Vessel Cyber Risk Management Work Instruction*.[32] This process would continue to be the Coast Guard's primary means of ensuring cybersecurity readiness on foreign-flagged vessels, which are exempt from this proposed rule.

If your facility or vessel would be subject to this proposed rule and you view a portion of it as redundant with the requirements of another Federal agency, please let us know. We seek to eliminate any unnecessary redundancies.

Section 101.610—Federalism.

We discuss the purpose and contents of this proposed section in section VI.E, *Federalism*, in this preamble.

Section 101.615—Definitions.

[32] See footnote 12.

This section lists new cybersecurity related definitions the Coast Guard proposes to include in 33 CFR part 101, in addition to the maritime security definitions in 33 CFR 101.105. These definitions explain concepts relevant to cybersecurity and would help eliminate uncertainty in referencing and using these terms in 33 CFR part 101.

The Coast Guard consulted several authoritative sources for these proposed new definitions. These sources include Executive Order 14028, 6 U.S.C. 148, and the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (the Act).[33]

Another source for definitions is the "Vocabulary" page on CISA's National Initiative for Cybersecurity Careers and Studies website,[34] which is an online Federal resource for cybersecurity training and education. The Coast Guard also reviewed NIST's Computer Security Resource Center (CSRC).[35] NIST maintains CSRC to educate the public on computer security, cybersecurity, information security, and privacy. Definitions from CISA and NIST are authoritative sources in areas related to technology and cybersecurity.

In addition, the Coast Guard proposes to define the term *cybersecurity risk* consistent with the definition at section 2200 of the Homeland Security Act of 2002 (Pub. L. 107-296), as amended, *see* 6 U.S.C. 650(7). The Coast Guard notes, however, that it does not believe paragraph (b) of subsection 2200(7), which contains an exception for actions that solely involve a "violation of a consumer term of service or a consumer licensing agreement" is relevant to the facilities and vessels that are the subject of this rulemaking. Nevertheless, for consistency with the definition found in the Homeland Security Act and the sake of completeness, we have elected to include the complete

---

[33] Pub. L. 117-263, Sec. 11224(a)(1) (2022).
[34] National Initiative for Cybersecurity Careers and Studies, *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases*, https://niccs.cisa.gov/cybersecurity-career-resources/glossary, accessed September 15, 2023.
[35] CSRC, https://csrc.nist.gov/glossary, accessed September 15, 2023.

definition in this proposal. See also 46 U.S.C. 70101(2); Pub. L. 115-254, sec. 1805(b)(2).

The Coast Guard proposes to include definitions for *Cyber incident*, *Cyber risk*, *Cyber threat*, and *Cybersecurity vulnerability*. *Cyber incident* would relate to *Information Systems* and would be inclusive of both *Information Technology* and *Operational Technology*, all of which the Coast Guard is also proposing to define. The Coast Guard also proposes new defined terms that are applicable to maritime cybersecurity, including *Critical Information Technology or Operational Technology systems*, *Cyber Incident Response Plan*, *Cybersecurity Officer* or *CySO*, and *Cybersecurity Plan*. A CySO, for example, would be the person(s) responsible for developing, implementing, and maintaining cybersecurity portions of the VSP, FSP, or OCS FSP. The CySO would also act as a liaison with the Captain of the Port (COTP) and company, vessel, and facility security officers.

In addition, the Coast Guard welcomes comments on whether we should define and use the term *Reportable cyber incident*. The proposed definition of a *reportable cyber incident* would be based on the Cyber Incident Reporting Council's model definition in DHS's Report to Congress of September 19, 2023.[36] If adopted, the term *reportable cyber incident* would replace *cyber incident* in proposed §§ 101.620(b)(7) and 101.650(g)(1). Specifically, a reportable cyber incident would mean an incident that leads to, or, if still under investigation, could reasonably lead to any of the following:

(1) Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system;

(2) Disruption or significant adverse impact on the reporting entity's ability to engage in business operations or deliver goods or services, including those that have a

[36] *See* DHS Office of Strategy, Policy, and Plans, Harmonization of Cyber Incident Reporting to the Federal Government (Sept. 19, 2023), https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government, accessed Sept. 19, 2023.

potential for significant impact on public health or safety or may cause serious injury or death;

(3) Disclosure or unauthorized access directly or indirectly of non-public personal information of a significant number of individuals;

(4) Other potential operational disruption to critical infrastructure systems or assets; or

(5) Incidents that otherwise may lead to a TSI as defined in 33 CFR 101.105.

The Coast Guard's existing regulations in 33 CFR part 101 require regulated entities to report suspicious activity that may result in a TSI, breaches of security, and TSIs involving computer systems and networks. *See* 33 CFR 101.305. The purpose of defining a reportable cyber incident in this NPRM is to establish a threshold between the cyber incidents that must be reported and the ones that do not. We request public comment on the substance of this definition, its elements, potential burden on industry, as well as the need and effectiveness of including it in this regulation. We also invite comments on whether we should define any terms we use in the proposed rule that are not defined in proposed § 101.615.

In this NPRM, the Coast Guard is also seeking comments on two alternative potential regulatory measures for reporting cyber incidents. In the first alternative, the Coast Guard would require that reportable cyber incidents would be reported to the National Response Center (NRC) without delay to the telephone number listed in 33 CFR 101.305(a). Cyber incidents with no physical or pollution effects could also be reported directly to CISA via report@cisa.gov or 1-888-282-0870. All such reports would be shared between the NRC and CISA Central and satisfy the requirement to report to the Coast Guard.

In the second alternative, the Coast Guard seeks comments on whether it should require that reportable cyber incidents be reported to CISA. While this alternative would

be a change from current practice, it could allow more efficient use of DHS' cybersecurity resources and may advance the cybersecurity vision laid out by Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which will be implemented by regulations that are still under development. Information submitted to CISA would be shared with the Coast Guard, ensuring continued efficient responses.

If we were to use either alternative, to the extent that the reporting obligation imposed by this NPRM constitutes a requirement to report "substantially similar information . . . within a substantially similar timeframe" when compared to a rule implementing CIRCIA, covered entities may be excused from any duplicative reporting obligations under the CIRCIA rulemaking.[37] In line with that provision, we invite your comments on whether we should expressly require reporting of ransom payments in connection with ransomware attacks. We request comment on whether we should use either of these two alternatives in a final rule.

Section 101.620—Owner or Operator

This proposed section would require each owner and operator of a U.S.-flagged vessel, facility, or OCS facility to assign qualified personnel to develop a Cybersecurity Plan and ensure the Cybersecurity Plan incorporates detailed preparation, prevention, and response activities for cybersecurity threats and vulnerabilities.

Additional responsibilities of owners and operators of U.S.-flagged vessels, facilities, and OCS facilities would include:

- Designating a CySO, in writing, by name and title, and identifying how the CySO can be contacted at any time. A CySO would have to be accessible to the Coast Guard 24 hours a day, 7 days a week (see proposed § 101.620(b)(3));

[37] *See* 6 U.S.C. 681b(a)(5)(B) (exception to reporting requirements for certain substantially similar reporting requirements "where the Agency has an agreement in place that satisfies the requirements of section 681g(a) of this title").

- Ensuring that a Cybersecurity Assessment is conducted annually or sooner, under the circumstances described in this NPRM (see proposed §§ 101.620(b)(4) and 101.650(e)(1));
- Ensuring that a Cybersecurity Plan is developed and submitted for Coast Guard approval, either as a separate document or as an addition to an existing FSP, VSP, or OCS FSP (see proposed §§ 101.620(b)(1) and 101.630(a));
- Operating the U.S.-flagged vessel, facility, or OCS facility in accordance with the approved Cybersecurity Plan (see proposed § 101.620(b)(5)); and
- Reporting all cyber incidents, including TSIs, to the NRC and relevant authorities according to the Cybersecurity Plan (see proposed §§ 101.305 and 101.620(b)(7)).

Section 101.625—Cybersecurity Officer

The CySO may be a full-time, collateral, or contracted position. The same person may serve as the CySO for more than one vessel, facility, or OCS facility. The CySO would need to have general knowledge of a range of issues relating to cybersecurity, such as cybersecurity administration, relevant laws and regulations, current threats and trends, risk assessments, inspections, control procedures, and procedures for conducting exercises and drills. When considering assignment of the CySO role to the existing security officer, the owner or operator should consider the depth and scope of these new responsibilities in addition to existing security duties.

The most important duties a CySO would perform include ensuring development, implementation, and finalization of a Cybersecurity Plan; auditing and updating the Plan; ensuring adequate training of personnel; and ensuring the U.S.-flagged vessel, facility, or OCS facility is operating in accordance with the Plan and in continuous compliance with this subpart. The CySO would have the authority to assign cybersecurity duties to other personnel; however, the CySO would remain responsible for the performance of these duties.

Section 101.630—Cybersecurity Plan

This proposed section contains minimum requirements for the Cybersecurity Plan. The Cybersecurity Plan would be maintained consistent with the recordkeeping requirements in 33 CFR 104.235 for vessels, 33 CFR 105.225 for facilities, and 33 CFR 106.230 for OCS facilities. *See* proposed § 101.640. A Cybersecurity Plan would incorporate the results of a Cybersecurity Assessment and consider the recommended measures appropriate for the U.S.-flagged vessel, facility, or OCS facility. A Cybersecurity Plan could be combined with or complement an existing FSP, VSP, or OCS FSP. A Cybersecurity Plan could be kept in an electronic format if it can be protected from being deleted, destroyed, overwritten, accessed, or disclosed without authorization.

The format of a Cybersecurity Plan required under this proposed rule would include the following individual sections:

(1) Cybersecurity organization and identity of the CySO (see proposed § 101.625 Cybersecurity Officer);

(2) Personnel training (see proposed § 101.625 (d)(8), (9) Cybersecurity Officer);

(3) Drills and exercises (see proposed § 101.635 Drills and Exercises);

(4) Records and documentation (see proposed § 101.640 Records and Documentation);

(5) Communications (see proposed § 101.645 Communications);

(6) Cybersecurity systems and equipment with associated maintenance; (see proposed § 101.650(e)(3) Cybersecurity Measures: Routine Maintenance);

(7) Cybersecurity measures for access control, including computer, IT, and OT areas (see proposed § 101.650(a) Cybersecurity Measures: Account Measures);

(8) Physical security controls for IT and OT systems (see proposed § 101.650(i) Cybersecurity Measures: Physical Security);

(9) Cybersecurity measures for monitoring (see proposed § 101.650(f) Cybersecurity Measures: Supply Chain; (h) Network Segmentation; (i) Physical Security);

(10) Audits and amendments to the Cybersecurity Plan (see proposed § 101.630(f) Cybersecurity Plan: Audits);

(11) Cybersecurity audit and inspection reports to include documentation of resolution or mitigation of all identified vulnerabilities (see proposed § 101.650(e) Cybersecurity Measures: Risk Management);

(12) Documentation of all identified unresolved vulnerabilities to include those that are intentionally unresolved due to risk acceptance by the owner or operator (see proposed § 101.650(e) Cybersecurity Measures: Risk Management);

(13) Cyber incident reporting procedures in accordance with part 101 of this subchapter (see proposed § 101.650(g) Cybersecurity Measures: Resilience); and

(14) Cybersecurity Assessment (see proposed § 101.650(e) Cybersecurity Measures: Risk Management).

Depending on operational conditions and cybersecurity risks, the owner or operator may develop a Cyber Incident Response Plan as a separate document or as an addition to the Cybersecurity Plan.

Submission and Approval of the Cybersecurity Plan

An owner or operator would submit a Cybersecurity Plan for review to the cognizant COTP or the Officer in Charge, Marine Inspections (OCMI) for U.S. facilities and OCS facilities, or to the U.S. Coast Guard's Marine Safety Center (MSC) for U.S.-flagged vessels. *See* proposed § 101.630(d). A letter certifying that the Plan meets the requirements of this subpart must accompany the submission. Once the COTP or MSC finds that the Plan meets the cybersecurity requirements in § 101.630, they would send a

letter to the owner or operator approving the Cybersecurity Plan or approving the Plan under certain conditions.

If the cognizant COTP, OCMI, or MSC requires additional time to review the Plan, they would have the authority to return a written acknowledgement to the owner or operator stating that the Coast Guard will review the Cybersecurity Plan submitted for approval, and that the U.S.-flagged vessel, facility, or OCS facility may continue to operate as long as it remains in compliance with the submitted Cybersecurity Plan. *See* proposed § 101.630(d)(1)(iv).

If the COTP, OCMI, or MSC finds that the Cybersecurity Plan does not meet the requirements in § 101.630, the Plan would be returned to the owner or operator with a letter explaining why the Plan did not meet the requirements. The owner or operator will have at least 60 days to amend the Plan and cure deficiencies outlined in the letter. Until the amendments are approved, the owner or operator must ensure temporary cybersecurity measures are implemented to the satisfaction of the Coast Guard. *See* proposed § 101.630(e)(1)(ii).

Deficiencies would have to be corrected, and the Plan would have to be resubmitted for approval within the time period specified in the letter. If the owner or operator fails to cure those deficiencies within 60 days, the Plan would be declared noncompliant with these proposed regulations and other relevant regulations in title 33 of the CFR. If the owner or operator disagrees with the deficiency determination, they would have the right to appeal or submit a petition for reconsideration or review to the respective COTP, District Commander, OCMI, or MSC per § 101.420.

Under proposed § 101.650(e)(1), a cybersecurity assessment would have to be conducted when one or both of the following situations occurs:

- There is a change in ownership of a U.S.-flagged vessel, facility, or an OCS facility; or

- There are major amendments to the Cybersecurity Plan.

Each owner or operator would determine what constitutes a "major amendment" as appropriate for their organization based on types of changes to their security measures and operational risks. When submitting proposed amendments to the Coast Guard, either after a cybersecurity assessment or at other times, you would not be required to submit the Cybersecurity Plan with the proposed amendment. Under § 101.630(f)(1), the CySO must ensure that an audit of the Cybersecurity Plan and its implementation is performed annually, beginning no later than 1 year from the initial date of approval. Additional audits would need to be conducted if there is a change in ownership or modifications of cybersecurity measures, but such audits may be limited to sections of the Plan affected by the modification. See proposed § 101.630(f)(2) and (3). Those conducting an internal audit must have a level of knowledge and independence specified in § 101.630(f)(4). Under § 101.630(f)(5), if the results of the audit require the Cybersecurity Plan to be amended, the CySO must submit the proposed amendments to the Coast Guard for review within 30 days of completing the audit.

Section 101.635—Drills and Exercises

Under this proposed section, cybersecurity drills and exercises would be required to test the proficiency of U.S.-flagged vessel, facility, and OCS facility personnel in assigned cybersecurity duties and in the effective implementation of the VSP, FSP, OCS FSP, and Cybersecurity Plan. Drills and exercises would also enable the CySO to identify any related cybersecurity deficiencies that need to be addressed.

Cybersecurity drills would generally test an operational response of at least one specific element of the Cybersecurity Plan, as determined by the CySO, such as access control for a critical IT or OT system, or network scanning. A drill would be required at least once every 3 months and may be held in conjunction with other drills, if appropriate.

Cybersecurity exercises are a full test of an organization's cybersecurity regime and would include substantial and active participation of cybersecurity personnel. The participants may include local, State, and Federal Government personnel. Cybersecurity exercises would generally test and evaluate the organizational capacity to manage a combination of elements in the Cybersecurity Plan, such as detecting, responding to, and mitigating a cyber incident.

The exercises would be required at least once each calendar year, with no more than 18 months between exercises. Exercises may be specific to a facility, OCS facility, or a U.S.-flagged vessel, or may serve as part of a cooperative exercise program or port exercises. The exercises for the Cybersecurity Plans could be combined with other required security exercises, if appropriate.

The proposed drill or exercise requirements specified in this section may be satisfied by implementing cybersecurity measures required by the VSP, FSP, OCS FSP, and Cybersecurity Plan after a cyber incident, as long as the vessel, facility, or OCS facility achieves and documents the drill and exercise goals for the cognizant COTP or MSC. Any corrective action must be addressed and documented as soon as possible.

Section 101.640—Records and Documentation

This proposed section would require owners and operators to follow the recordkeeping requirements in 33 CFR 104.235 for vessels, 33 CFR 105.225 for facilities, and 33 CFR 106.230 for OCS facilities. For example, records must be kept for at least 2 years and be made available to the Coast Guard upon request. The records can be kept in paper or electronic format and must be protected against unauthorized access, deletion, destruction, amendment, and disclosure. Records that each vessel, facility, or OCS facility keep would vary because each organization would maintain records specific to their operations. At a minimum, the records would have to capture the following activities: training, drills, exercises, cybersecurity threats, incidents, and audits of the

Cybersecurity Plan as set forth in the cited recordkeeping requirements above and made applicable to records under this subpart per § 101.640.

Section 101.645—Communications

This proposed section would require the CySO to maintain an effective means of communication to convey changes in cybersecurity conditions to the personnel of the U.S.-flagged vessel, facility, or OCS facility. In addition, the CySO is required to maintain an effective and continuous means of communicating with their security personnel, U.S.-flagged vessels interfacing with the facility or OCS facility, the cognizant COTP, and national and local authorities with security responsibilities.

Section 101.650—Cybersecurity Measures

This section proposes specific cybersecurity measures to identify risks, detect threats and vulnerabilities, protect critical systems, and recover from cyber incidents. Any intentional gaps in cybersecurity measures would be documented as accepted risks under proposed § 101.630(c)(12). If the owner or operator is unable to comply with the requirements of this subpart, they may seek a waiver or an equivalence determination under proposed § 101.665.

A discussion of each component of proposed § 101.650 follows.

Section 101.650 paragraph (a): Account security measures.

This paragraph would identify minimum account measures to protect critical IT and OT systems from unauthorized cyber access and limit the risk of a cyber incident. Access control is a foundational category and is highlighted as a "Protect" function of NIST's Cybersecurity Framework (CSF).[38] Existing regulations in §§ 104.265, 105.255 through 105.260, and 106.260 through 106.265 prescribe control measures to limit access to restricted areas and detect unauthorized introduction of devices capable of damaging U.S.-flagged vessels, U.S. facilities, OCS facilities, or ports. This proposed provision is

[38] NIST CSF, www.nist.gov/cyberframework/protect, accessed July 18, 2023.

derived from NIST's standards mentioned earlier for the cyber domain and establish minimum account security measures to manage credentials and secure access to critical IT and OT systems. We invite your comments on the minimal requirements proposed in § 101.650(a).

Account security measures for cybersecurity would include lockouts on repeated failed login attempts, password requirements, multifactor authentication, applying the principle of least privilege to administrator or otherwise privileged accounts, and removing credentials of personnel no longer associated with the organization. Numerous consensus standards that are generally accepted employ similar requirements.[39] Together, these provisions would mitigate the risks of brute force attacks, unauthorized access, and privilege escalation. The owner or operator would be responsible for implementing and managing these account security measures, including ensuring that user credentials are removed or revoked when a user leaves the organization. The CySO would ensure documentation of such measures in Section 7 of the Cybersecurity Plan.

Section 101.650 paragraph (b): Device security measures.

This paragraph would provide specific proposed requirements to mitigate risks and vulnerabilities in critical IT and OT systems and equipment. With increased connectivity to public internet, networks on U.S.-flagged vessels, U.S. facilities, and OCS facilities have an expansive attack surface. These provisions would reduce the risks of unauthorized access, malware introduction, and service interruption. This paragraph would apply the "Identify" function of the NIST CSF.[40] Existing regulations in 33 CFR 104.265, 105.255 through 105.260, and 106.260 through 106.265 are similar. For example, § 105.260 limits access to areas that require a higher degree of protection.

---

[39] *See*, for example, NIST CSF: PR.AC, CIS Controls 1, 12, 15, 16, and COBIT DSS05.04, DSS05.10, DSS06.10, and ISA 62443-2-1.

[40] NIST CSF; Identify, "NIST Cybersecurity Publication by Category," *Asset Management ID.AM*, updated May 3, 2021, www.nist.gov/cyberframework/identify, accessed July 18, 2023. NIST Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020, page 107, https://doi.org/10.6028/NIST.SP.800-53r5, accessed August 24, 2023.

Proposed paragraph (b) would also require owners and operators to designate critical IT and OT systems.[41] Developing and maintaining an accurate inventory and network map would reduce the risk of unknown or improperly managed assets. The Cybersecurity Plan would also govern device management. The CySO would maintain the network map and develop and maintain the list of approved hardware, software, and firmware. In addition to identifying risks, these provisions would aid in the proper lifecycle management of assets, including patching and end-of-life management. These requirements are foundational to many industry consensus standards and would reinforce Coast Guard regulations to protect communication networks.

Section 101.650 paragraph (c): Data security measures.

This paragraph would prescribe fundamental data security measures that stem from the "Protect" function of the NIST CSF. Data security measures protect personnel, financial, and operational data and are consistent with basic risk management activities of the maritime industry. The IMO recognizes the importance of risk management related to data security on U.S.-flagged vessels,[42] and the Coast Guard previously highlighted data security measures in its policy for MTSA-regulated U.S. facilities.[43]

Data security measures prevent data loss and aid in detection of malicious activity on critical IT and OT systems. The fundamental measures proposed here would establish baseline protections upon which owners and operators could build. This paragraph

---

[41] To help CySOs identify which systems are critical, the Coast Guard's Office of Port and Facility Compliance (CG-FAC) has published maritime specific CSF profiles on its homepage at www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Port-Facility-Compliance/Domestic-Ports-Division/cybersecurity/, accessed July 18, 2023 and in pages 20 through 24 of Appendix A, Maritime Bulk Liquid Transfer Profile at https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.dco.uscg.mil%2FPortals%2F9%2FCG-FAC%2FDocuments%2FCyber%2520Profiles%2520Overview.docx%3Fver%3D2018-01-10-143126-467&wdOrigin=BROWSELINK, accessed July 18, 2023.

[42] MSC-FAL.1/Circ.3/Rev.1: "Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations."

[43] NVIC 01-20 at page 2: "Each facility should also determine how, and where, its data is stored and, if it is stored offsite, whether the data has a critical link to the safety and/or security functions of the facility. If such a critical link exists, the facility should address any vulnerabilities . . . . "

would require data logs to be securely captured, stored, and protected so that they are accessible only by privileged users, and would require encryption for data in transit and data at rest. CySOs would rely on generally accepted industry standards and risk management principles to determine the suitability of specific encryption algorithms for certain purposes, such as protecting critical IT and OT data with a more robust algorithm than for routine data.[44] A CySO would establish more detailed data security policies in Section 9 of the Cybersecurity Plan. Those policies would be adapted to the unique operations of the U.S.-flagged vessel, facility, or OCS facility.

Section 101.650 paragraph (d): Cybersecurity training for personnel.

This paragraph would specify proposed cybersecurity training requirements. Security training is a vital aspect of the MTSA. Relevant provisions in 33 CFR already require all personnel to have knowledge, through training or equivalent job experience, in the "Recognition and detection of dangerous . . . devices."[45] Since 2020, the Coast Guard has interpreted this requirement to include relevant cybersecurity training.[46] While formal training may be appropriate, the Coast Guard is not proposing to mandate a format of training. However, the training would have to, at minimum, cover relevant provisions of the Cybersecurity Plan to include recognizing, detecting, and preventing cybersecurity threats; and reporting cyber incidents to the CySO.

The types of training would also need to be consistent with the roles and responsibilities of personnel, including access to critical IT and OT systems and operating network-connected machineries. Key cybersecurity personnel and management would need to have current knowledge of threats to deal with potential

---

[44] *See*, for example, ISA 62443-3-3, CIS CSC 13, 14 in the EDM NIST Cybersecurity Framework Crosswalks, available at www.cisa.gov/sites/default/files/publications/4_NIST_CSF_EDM_Crosswalk_v3_April_2020.pdf, accessed July 18, 2023.

[45] 33 CFR 104.225(c) (Vessels), 105.215(c) (Facilities), and 106.220(c) (OCS Facilities).

[46] NVIC 01-20 ENCL(1) at page 3: "Describe how cybersecurity is included as part of personnel training, policies, and procedures, and how this material will be kept current and monitored for effectiveness."

cyber-attacks and understand procedures for responding to a cyber incident. The owner, operator, or CySO would ensure all personnel designated by the CySO complete the core training within 5 days of gaining system access, but no later than 30 days after hiring, and annually thereafter, and that key personnel receive specialized training annually or more frequently as needed. Existing personnel would be required to receive training on relevant provisions of the Cybersecurity Plan within 60 days of the Plan being approved, and for all other required training within 180 days of the effective date of a final rule, and annually thereafter. (See § 101.650(d)(3)).

Section 101.650 paragraph (e): Risk Management.

This paragraph would establish three levels of Cybersecurity Assessment and risk management: (1) conducting annual Cybersecurity Assessments; (2) completing penetration testing upon renewal of a VSP, FSP, or OCS FSP; and (3) ensuring ongoing routine system maintenance. The CySO would ensure that these activities, which are listed in Sections 11 and 12 of the Cybersecurity Plan, are documented and completed.

Following a Cybersecurity Assessment, the CySO would incorporate feedback from the assessment into the Cybersecurity Plan through an amendment to the Plan. A Cybersecurity Assessment would be conducted within 1 year from the effective date of a final rule and annually thereafter. The Assessment must be conducted sooner than annually in the following circumstances:

- There is a change in ownership of a U.S.-flagged vessel, facility, or an OCS facility; or
- There are major events requiring amendments to the Cybersecurity Plan.

While Cybersecurity Assessments provide a valuable picture of potential security weaknesses, penetration tests can add additional context by demonstrating whether malicious actors could leverage those weaknesses. Penetration tests can also help prioritize resources based on what poses the most risk. Routine system maintenance

requires an ongoing effort to identify vulnerabilities and would include scanning and reviewing known exploited vulnerabilities (KEVs) by documenting, tracking, and monitoring them. These proposed provisions would mirror the security system and equipment maintenance requirements in 33 CFR 104.260 for vessels, 33 CFR 105.250 for facilities, and 33 CFR 106.255 for OCS facilities, and reflect the Coast Guard's longstanding view on cybersecurity. To improve risk management across the maritime sector, CySOs would establish, subject to any applicable antitrust law limitations,[47] information-sharing procedures for their organizations, which would include procedures to receive and act on KEVs, as well as methods for sharing threat and vulnerability information.

The "Protect" function of the NIST CSF emphasizes the importance of strong processes and procedures for protecting information.[48] For example, organizations would have to ensure information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Risk management is key in protecting IT and OT components that may include cybersecurity vulnerabilities in their design, code, or configuration.

Owners and operators may use information-sharing services or organizations such as an Information Sharing and Analysis Center or an Information Sharing and Analysis Organization. The Coast Guard would not endorse specific information-sharing organizations, so owners and operators would be free to use information-sharing organizations to suit their needs.[49] Industry consensus standards provide generally

---

[47] The sharing of competitively sensitive information between or among competitors raises antitrust concerns. For example, information sharing is not exempted under the Cybersecurity Information Sharing Act of 2015 if the information shared results in price fixing, market allocation, boycotting, monopolistic conduct, or other collusive conduct.

[48] NIST CSF Internal Controls, Appendix A, Table A-1, PR.IP-12, page 261, link.springer.com/content/pdf/bbm:978-1-4842-3060-2/1.pdf, accessed July 18, 2023.

[49] The Coast Guard encourages CySOs to explore resources through CGCYBER Maritime Cyber Readiness Branch, available at https://www.uscg.mil/MaritimeCyber/; *see also* CISA's "Information Sharing and Awareness," available at https://www.cisa.gov/information-sharing-and-awareness, accessed July 18, 2023.

accepted techniques that sanitize and reduce attribution to information to ensure information sharing does not compromise proprietary business information.[50] In addition, regardless of the services or organizations used, owners and operators should comply with applicable antitrust laws and should not share competitively sensitive information, such as price or cost data, that can result in unlawful price-fixing, market allocation, or other forms of competitor collusion. Use of any information-sharing services or organizations would not meet or replace reporting requirements under 33 CFR 101.305.

The Coast Guard emphasized its commitment to helping maritime industry stakeholders identify and address vulnerabilities in its *2021 Cyber Trends and Insights in the Marine Environment* report.[51] In that report, the Coast Guard highlighted additional resources that CySOs should leverage to manage cybersecurity vulnerabilities.

Section 101.650 paragraph (f): Supply chain.

This proposed paragraph would include provisions to specify measures to manage cybersecurity risks in the supply chain. Legitimate third-party contractors and vendors may inadvertently provide a means of attack or vectors that allow malicious actors to exploit vulnerabilities within the supply chain. Section 1.1 of the NIST CSF emphasizes managing cybersecurity risks in the supply chain as part of the "Identify" function.[52]

Under this proposed paragraph, the owner, operator, or CySO would ensure that measures to manage cybersecurity risks in the supply chain are in place to mitigate the risks associated with external parties. These measures would include considering

---

[50] *See, e.g.*, NIST Special Publication 800-150, "Guide to Cyber Threat Information Sharing," Johnson et al, October 2016, nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-150.pdf, accessed July 18, 2023.
[51] "2021 Cyber Trends and Insights in the Marine Environment," August 5, 2022, https://www.dco.uscg.mil/Portals/9/2021CyberTrendsInsightsMarineEnvironmentReport.pdf.
[52] NIST CSF, Version 1.1, "ID.SC: Supply Chain Risk Management," https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-sc/, accessed July 18, 2023.

cybersecurity capabilities in selecting vendors, establishing procedures for information sharing and notifying relevant parties, and monitoring third-party connections.

Through their contractual agreements, vendors would ensure the integrity and security of software and hardware, such as software releases and updates, notifications, and mitigations of vulnerabilities. These provisions would establish a minimum level of CRM within the supply chain. Industry standards provide additional measures.[53] The IMO also recognizes that cybersecurity risks in the supply chain, and these provisions would align with the guidelines and recommendations referenced in MSC-FAL Circ. 3/Rev.1.[54]

Section 101.650 paragraph (g): Resilience.

This paragraph proposes a few key activities to ensure that U.S.-flagged vessels, facilities, and OCS facilities can recover from major cyber incidents with minimal impact to critical operations. Provisions under response and recovery can help an organization recover from a cyber-attack and restore capabilities and services.

This proposed rule would require the owner, operator, or CySO to ensure the following response and recovery activities: report any cyber incidents to the Coast Guard; develop, implement, maintain, and exercise the Cyber Incident Response Plan; periodically validate the effectiveness of the Cybersecurity Plan; and perform backups of critical IT and OT systems. The Coast Guard would accept review of a cyber incident as meeting the periodic validation requirement in § 101.650(g).

In addition, the NIST CSF describes numerous provisions within the "Recover" function aimed at improving response and recovery.[55] The IMO also notes resilience.[56]

---

[53] *See*, for example, NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," May 2022, https://doi.org/10.6028/NIST.SP.800-161r1, accessed July 18, 2023.
[54] MSC-FAL.1/Circ.3/Rev.1, 2.1.6 and 4.2; see footnote 28.
[55] NIST CSF, Version 1.1 "RC: Recover," https://csf.tools/reference/nist-cybersecurity-framework/v1-1/rc/, accessed July 19, 2023.
[56] MSC-FAL Circ. 3/Rev. 1, 3.5.5; see footnote 28.

Section 101.650 paragraph (h): Network segmentation.

This paragraph would require a CySO to ensure the network is segmented and to document those activities in the Cybersecurity Plan. Network integrity is a key provision under the "Protect" function of the NIST CSF.[57] Network architectures vary widely based on the operations of a vessel or facility. Separating IT and OT networks is challenging, and it becomes increasingly difficult with an increase in the various devices connected to the network. Network segmentation ensures valuable information is not shared with unauthorized users and decreases damage that can be caused by malicious actors. Nonetheless, the Coast Guard recognizes that the IT and OT interface represents a weak link. Industry standards in this area are evolving, and it is an area that NIST continues to research.[58]

Section 101.650 paragraph (i): Physical security.

This paragraph would specify that, along with the cybersecurity provisions proposed for inclusion in this part, owners, operators, and CySOs would manage physical access to IT and OT systems. As described in the "Protect" function of the NIST CSF, physical security protects critical IT and OT systems by limiting access to the human-machine interface (HMI).[59] Physical security measures proposed here would supplement the existing vessel security assessment (VSA), FSA, and OCS FSA requirements in 33 CFR 104.270 for vessels, 33 CFR 105.260 for facilities, and 33 CFR 106.260 for OCS facilities. Similarly, under this proposed paragraph, the CySO would designate areas restricted to authorized personnel and secure HMIs and other hardware. Also under this proposed paragraph, the CySO would establish policies to restrict the use of unauthorized

---

[57] NIST CSF, Version 1.1, "PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)." csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ac/pr-ac-5/, accessed July 19, 2023.

[58] *See* NIST Special Publication 800-82r3," Guide to Operational Technology (OT) Security," draft published April 26, 2022; doi.org/10.6028/NIST.SP.800-82r3.ipd, accessed July 19, 2023.

[59] NIST CSF, Version 1.1, "PR.AC-2: Physical Access to Assets is Managed and Protected." csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ac/pr-ac-2/, accessed July 19, 2023.

media and hardware. These proposed provisions would mirror existing Coast Guard policy outlined in NVIC 01-20.[60]

Section 101.655—Cybersecurity Compliance Dates.

This proposed section would state that a Cybersecurity Plan as required by this proposed rule would be made available to the Coast Guard for review during the second annual audit of the existing, approved VSP, OCS FSP, or FSP after the effective date of a final rule, as required by 33 CFR 104.415 for vessels, 33 CFR 105.415 for facilities, and 33 CFR 106.415 for OCS facilities. The intent of this proposed implementation period is to allow adequate time for owners and operators to develop a Cybersecurity Plan.

Section 101.660—Cybersecurity Compliance Documentation.

This proposed section would allow the Coast Guard to verify an approved Cybersecurity Plan for U.S.-flagged vessels, facilities, and OCS facilities. Each owner or operator would ensure that the cybersecurity portion of their Plan and penetration test results are available to the Coast Guard upon request.

Section 101.665—Noncompliance, Waivers, and Equivalents.

This proposed section would provide the opportunity for waiver and equivalence determinations for owners and operators when they are unable to meet the requirements in subpart F, as outlined in 33 CFR 104.130, 104.135, 105.130, 105.135, and 106.130, to include the cybersecurity regulations proposed in this NPRM. It would also expand temporary permission provisions in 33 CFR 104.125, 105.125, and 106.120.

Section 101.670—Severability.

This proposed section would reflect the Coast Guard's intent that the provisions of subpart F be considered severable from each other to the greatest extent possible. For

[60] NVIC 01-20, enclosure (1), at page 4: "Security measures for access control 33 CFR 105.255 and 106.260 Establish security measures to control access to the facility. This includes cyber systems that control physical access devices such as gates and cameras, as well as cyber systems within secure or restricted areas, such as cargo or industrial control systems. Describe the security measures for access control." (85 FR 16108).

instance, if a court of competent jurisdiction were to hold that the rule or a portion thereof may not be applied to a particular owner or operator or in a particular circumstance, the Coast Guard would intend for the court to leave the remainder of the rule in place with respect to all other covered persons and circumstances. The inclusion of a severability clause in subpart F would not be intended to imply a position on severability in other Coast Guard regulations.

Inviting Comments on Regulatory Harmonization

As noted by the Office of the National Cyber Director in an August 2023 Request for Information,[61] the National Cybersecurity Strategy[62] calls for establishing cybersecurity regulations to secure critical infrastructure where existing measures are insufficient, harmonizing[63] and streamlining new and existing regulations, and enabling regulated entities to afford to achieve security.

The Coast Guard emphasizes its commitment to regulatory harmonization and streamlining, and notes that this proposed rule, which is grounded in NIST's Framework for Improving Critical Infrastructure Cybersecurity, NIST's standards and best practices, and CISA's CPGs, is consistent with such priorities. The Coast Guard also acknowledges the ongoing rulemakings of other DHS components, including ongoing rulemakings on cybersecurity in surface transportation modes[64] and implementation of CIRCIA.[65] The Coast Guard notes potential differences in terminology and policy as

---

[61] *See* 88 FR 55694 (Aug. 16, 2023).
[62] *See* The White House, National Cybersecurity Strategy (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.(accessed Sept. 19, 2023).
[63] As used in this context, "harmonization" refers to a common set of updated baseline regulatory requirements that would apply across sectors. Sector regulators such as the Coast Guard may appropriately go beyond the harmonized baseline to address cybersecurity risks specific to their sectors. *See* 88 FR at 55694.
[64] *See* TSA, Fall 2023 Unified Agenda, RIN 1652-AA74: Enhancing Surface Cyber Risk Management, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=1652-AA74 (accessed Jan. 19, 2024).
[65] *See* CISA, Fall 2023 Unified Agenda, RIN 1670-AA04: Cybersecurity Incident Reporting for Critical Infrastructure Act Regulations, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310&RIN=1670-AA04 (accessed Jan. 19, 2024).

compared to those rulemakings; although the Coast Guard views such differences as intentional and based on sector-specific distinctions, we welcome comments on opportunities to harmonize and streamline regulations where feasible and appropriate. Note that proposed § 101.665, Noncompliance, Waivers, and Equivalents, could offer stakeholders an option for requesting compliance that is harmonized with similar requirements.

Inviting Comments on whether to amend 33 CFR 160.202—Definitions

The Coast Guard invites comments on whether we should amend the definition of *hazardous condition* in 33 CFR 160.202 to help address current and emerging cybersecurity threats to the MTS. The amendment would likely add "cyber incident (as defined in § 101.615 of this chapter)," to other existing examples of hazardous conditions—such as collision, allision, fire, explosion, grounding, leaking, damage, and personnel injury. Although a hazardous condition as currently defined can already involve a cyber incident, this amendment would clearly link the definition of a hazardous condition to the concept of a cyber incident.

Under 33 CFR 160.216, the owner, agent, master, operator, or person in charge of a vessel must immediately notify the Coast Guard of certain hazardous conditions. A hazardous condition either on board the vessel or caused by the vessel or its operation would be reported by the vessels listed in 33 CFR 160.203. Under the existing regulations, this reporting requirement already applies to U.S. commercial service vessels and all foreign vessels that are bound for or departing from ports or places within the navigable waters of the United States.

If we amend the definition of *hazardous condition* in § 160.202, we would consider a cyber incident report under part 160 satisfied by those subject to 33 CFR part 101, subpart F, who report the incident consistent with § 101.620(b)(7). Given the variety of hazardous conditions, for response purposes, it is best that such conditions be

reported to the nearest Coast Guard Sector Office or Group Office. The Coast Guard would ensure that such officials are advised of relevant cyber incidents reported by vessels subject to 33 CFR part 101, subpart F.

VI. Regulatory Analyses

We developed this proposed rule after considering numerous statutes and Executive orders related to rulemaking. A summary of our analyses based on these statutes or Executive orders follows.

A. Regulatory Planning and Review

Executive Order 12866 (Regulatory Planning and Review), as amended by Executive Order 14094 (Modernizing Regulatory Review), and Executive Order 13563 (Improving Regulation and Regulatory Review), direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying costs and benefits, reducing costs, harmonizing rules, and promoting flexibility.

This proposed rule is a significant regulatory action under section 3(f) of Executive Order 12866, as amended by Executive Order 14094, but it is not significant under section 3(f)(1) because its annual effects on the economy do not exceed $200 million in any year of the analysis. Accordingly, OMB has reviewed this proposed rule. A regulatory impact analysis (RIA) follows.

In accordance with OMB Circular A-4 (available at www.whitehouse.gov/omb/circulars/), we have prepared an accounting statement showing the classification of impacts associated with this proposed rule.[66]

---

[66] The version of Circular A-4 issued November 9, 2023, is not effective until March 24, 2024. Therefore, this new version does not apply to this NPRM because this proposed rule was submitted to OIRA on November 13, 2023.

Agency/Program Office: U.S. Coast Guard

Rule Title: Cybersecurity in the Marine Transportation System

RIN#: 1625-AC77

Date: July 2023 (millions, 2022 dollars)

Table 1: OMB Circular A-4 Accounting Statement Categorizing Impacts for the Cybersecurity in the Marine Transportation System NPRM

Category	Primary Estimate		Minimum Estimate		High Estimate		Source
Benefits							
Annualized monetized benefits ($ Mil)	-	7%		7%		7%	RA
	-	3%		3%		3%	
Annualized quantified, but unmonetized, benefits							RA
Unquantifiable, qualitative Benefits	Reduce the risk of cyber incidents through enhanced detection and correction of vulnerabilities in IT and OT systems. Improve mitigation for the impacted entity and downstream economic participants if an incident occurs.						RA
	Improve protection of MTS firm and customer data to protect business operations, build consumer trust, and promote increased commerce in the U.S. economy.						
	Improve the minimum standard for cybersecurity to protect the MTS and avoid supply chain disruptions, which is vital to the U.S. economy and U.S. national security.						
Costs							
Annualized monetized costs ($ Mil)	$80.1	7%		7%		7%	RA
	$79.4	3%		3%		3%	RA
Annualized quantified, but unmonetized, costs	None						RA
Qualitative (un-quantified) costs	The unquantifiable costs of this proposed rule would be associated with the cyber risk mitigation actions identified as a result of this NPRM. These actions may involve changes to the physical security of hardware and physical access ports, network segmentation, the data space and encryption required for data backups and data logging measures, disabling applications running executable code, any necessary future software or hardware upgrades in addition to the incompatibility between older and newer software, and correcting vulnerabilities or issues identified during the implementation of this proposed rule.						RA
Transfers							
Annualized monetized transfers: “on budget”	N/A		N/A		N/A		RA
From whom to whom?	N/A						RA
Annualized monetized transfers: “off-budget”	N/A		N/A		N/A		
From whom to whom?	N/A		N/A		N/A		

Miscellaneous Analyses/Category		
Effects on Tribal, State, and/or local, governments	None	
Effects on small businesses	We conducted an initial Regulatory Flexibility analysis (IRFA) and estimate that this proposed rule may have a significant economic impact on a substantial number of small entities.	RA/IRFA
Effects on wages	None	
Effects on growth	Not measured	

The Coast Guard proposes to update its maritime security regulations by adding minimum cybersecurity requirements to 33 CFR part 101 for U.S.-flagged vessels subject to part 104, facilities subject to part 105, and OCS facilities subject to part 106. Specifically, this proposed rule would require owners or operators of U.S.-flagged vessels, facilities, and OCS facilities to develop an effective Cybersecurity Plan, which includes actions to prepare for, prevent, and respond to threats and vulnerabilities. One of these actions is to assign qualified personnel to implement the Cybersecurity Plan and all activities within the Plan. The Cybersecurity Plan would include: designating a CySO; conducting a Cybersecurity Assessment; developing and submitting the Plan to the Coast Guard for approval; operating a U.S.-flagged vessel, facility, and OCS facility in accordance with the Plan; implementing security measures based on new cybersecurity vulnerabilities; and reporting cyber incidents to the NRC, as defined in this preamble.

This proposed rule would further require owners and operators of U.S.-flagged vessels, U.S. facilities, and OCS facilities to perform cybersecurity drills and exercises in accordance with their VSP, FSP, and OCS FSP. Owners and operators of U.S.-flagged vessels, facilities, and OCS facilities would also be required to maintain records of cybersecurity related information in paper or electronic format.

Lastly, this proposed rule would require certain cybersecurity measures to identify risks, detect threats and vulnerabilities, protect critical systems, and to recover from cyber incidents. These measures include account security measures, device security measures,

data security measures, cybersecurity training for personnel, risk management, supply chain risk measures, penetration testing, resilience measures, network segmentation, and physical security.

Baseline Summary

The Coast Guard is not codifying existing guidance in this NPRM. The requirements of this proposed rule and the costs and benefits we estimate in this RIA would be new. The Coast Guard drafted the requirements of this proposed rule based on NIST's *Framework for Improving Critical Infrastructure Cybersecurity*, NIST's standards and best practices, and CISA's CPGs.

In February 2020, the Coast Guard issued NVIC 01-20, which provided clarity and guidance for MTSA-regulated facility and OCS facility owners and operators regarding existing requirements in the MTSA for computer systems and network vulnerabilities. However, the NVIC does not contain cybersecurity requirements for facility and OCS facility owners. Furthermore, the NVIC does not address the topic of cybersecurity for vessel owners and operators.

The IMO has issued other guidance on Cybersecurity in the past 6 years. In 2017, the IMO adopted resolution MSC.428(98) to the ISM Code on "Maritime Cyber Risk Management in Safety Management Systems (SMS)." Generally, this resolution states that an SMS should consider CRM and encourages Administrations to appropriately address cyber risks in an SMS by a certain date, in accordance with the ISM Code. In 2022, the IMO provided further guidance on maritime CRM in MSC-FAL.1/Circ.3-Rev.2, *Guidelines on Maritime Cyber Risk Management*, in an effort to raise the awareness about cybersecurity risks.

In addition, survey data indicates that some portions of the affected population of facility and OCS facility owners and operators are already implementing cybersecurity measures consistent with select provisions of the proposed rule, including 87 percent who

have implemented account security measures, 83 percent who have implemented multifactor authentication, 25 percent who have implemented annual cybersecurity training, and 68 percent who conduct penetration tests.[67] While we lack similar data on cybersecurity activities in the affected population of U.S.-flagged vessels, we acknowledge that it is likely that many owners and operators have implemented cybersecurity measures in response to private incentives and increasing cybersecurity risks over time. For the purposes of this analysis, however, we assume that owners and operators have no baseline cybersecurity activity, in the areas in which we lack data.

Estimated Costs of the Proposed Rule

We estimate the total discounted costs of this proposed rule to industry and the Federal Government to be approximately $562,740,969 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $80,121,654, using a 7-percent discount rate. See table 2.

Table 2: Total Estimated Costs of the Proposed Rule to Industry and Government (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facility and OCS Facility Costs	U.S.-flagged Vessel Costs	Government Costs	Total Costs	7 Percent	3 Percent
1	$33,469,773	$53,613,063	$351,638	$87,434,474	$81,714,462	$84,887,839
2	$37,053,260	$54,116,840	$16,921,067	$108,091,167	$94,411,011	$101,886,292
3	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$59,913,465	$67,168,260
4	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$55,993,893	$65,211,903
5	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$52,330,741	$63,312,527
6	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$48,907,234	$61,468,473
7	$25,788,807	$49,425,867	$4,301,574	$79,516,248	$49,518,723	$64,653,986
8	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$42,717,473	$57,939,931
9	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$39,922,872	$56,252,360
10	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$37,311,095	$54,613,942
Total	**$312,330,251**	**$439,884,727**	**$36,602,908**	**$788,817,886**	**$562,740,969**	**$677,395,513**

[67] In this analysis, the Coast Guard references a survey conducted by Jones Walker, a limited liability partnership (Jones Walker LLP). The title of the survey is "Ports and Terminals Cybersecurity Survey," which they conducted in 2022. This survey helped the Coast Guard to gain an understanding of the cybersecurity measures that are currently in place at facilities and OCS facilities in the United States. We cite relevant data from the survey when calculating industry costs throughout the regulatory analysis. Readers can access the survey at https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html; accessed July 19, 2023.

Annualized				**$78,881,789**	**$80,121,654**	**$79,411,419**

Note: Totals may not sum due to independent rounding.

We present a summary of the impacts of this proposed rule in table 3.

Table 3: Summary of Impacts of the Proposed Rule

Category	**Summary**
Applicability: Proposed new sections to 33 CFR part 101, subpart F—Cybersecurity	• Cybersecurity requirements for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities.
Affected Population	• Approximately 1,708 facility owners and operators of approximately 3,411 facilities. • Approximately 1,775 U.S.-flagged vessel owners and operators of approximately 10,286 U.S.-flagged vessels (5,473 U.S.-flagged vessels, excluding barges, where applicable).
Total Costs of the Proposed Rule (7-percent discount rate—all estimates in table)	**Costs to Industry:** Total discounted cost: $535,093,488 Annualized cost: $76,185,275 Total discounted cost to facilities and OCS facilities cost: $221,437,074 Annualized cost: $31,527,658 Total discounted cost to U.S.-flagged vessels: $313,656,415 Annualized cost: $44,657,617 **Costs to Federal Government:** Total discounted cost: $27,647,481 Annualized cost: $3,936,379 **Total Costs of Proposed Rule:** Total discounted cost: $562,740,969 Annualized cost: $80,121,654

Unquantified Costs	• Costs associated with the physical security of physical access ports and removable media. • Costs associated with network segmentation. • The cost of data encryption and acquiring data space needed to store data logs and backups. • Costs associated with disabling applications running executable code. • Costs associated with any future software or hardware upgrades needed to maintain system compatibility in the face of evolving cybersecurity threats. • Costs associated with the correction of vulnerabilities identified during the implementation of the provisions of the proposed rule.
Unquantified Benefits	• Reduce the risk of cyber incidents through enhanced detection and correction of vulnerabilities in IT and OT systems. Improve mitigation for impacted entities and downstream economic participants if an incident occurs. Improve protection of MTS firm and customer data to protect business operations, build consumer trust, and promote increased commerce in the U.S. economy. • Improve the minimum standard for cybersecurity to protect the MTS and avoid supply chain disruptions, which is vital to the U.S. economy and U.S. national security.

Affected Population

This proposed rule would affect owners and operators of U.S.-flagged vessels subject to 33 CFR part 104 (Maritime Security: Vessels), facilities subject to 33 CFR part 105 (Maritime Security: Facilities), and OCS facilities subject to 33 CFR part 106 (Marine Security: Outer Continental Shelf (OCS) Facilities). The Coast Guard estimates this proposed rule would affect approximately 10,286 vessels and 3,411 facilities (including OCS facilities).

The affected U.S.-flagged vessel population includes:

- U.S. towing vessels greater than 8 meters (26 feet) in registered length inspected under 46 CFR, subchapter M that are engaged in towing a barge or barges inspected under 46 CFR, subchapters D and O;

- U.S. tankships inspected under 46 CFR, subchapters D and O;
- U.S. barges inspected under 46 CFR, subchapters I (includes combination barges), D, and O, carrying certain dangerous cargo in bulk or barges and engaged on international voyages;
- Small U.S. passenger vessels carrying more than 12 passengers, including at least 1 passenger-for-hire, that are engaged on international voyages;
- Small U.S. passenger vessels inspected under 46 CFR, subchapter K that are certificated to carry more than 150 passengers;
- Large U.S. passenger vessels inspected under 46 CFR, subchapter H;
- Offshore supply vessels (OSVs) inspected under 46 CFR, subchapter L;
- Self-propelled U.S. cargo vessels greater than 100 gross register tons inspected under 46 CFR, subchapter I, except for commercial fishing vessels inspected under 46 CFR part 105; and
- U.S. MODUs and cargo or passenger vessels subject to SOLAS (1974), Chapter XI-1 or Chapter XI-2.

The affected facility population includes:

- Facilities subject to 33 CFR parts 126 (Handling of Dangerous Cargo at Waterfront Facilities) and 127 (Waterfront Facilities Handling Liquefied Natural Gas and Liquefied Hazardous Gas);
- Facilities that receive vessels certificated to carry more than 150 passengers, except vessels not carrying and not embarking or disembarking passengers at the facility;
- Facilities that receive vessels subject to SOLAS (1974), Chapter XI;
- Facilities that receive foreign cargo vessels greater than 100 gross register tons;
- Facilities that receive U.S. cargo vessels, greater than 100 gross register tons, inspected under 46 CFR, subchapter I, except facilities that receive only

commercial fishing vessels inspected under 46 CFR part 105; and

- Barge fleeting facilities that receive barges carrying, in bulk, cargoes regulated by 46 CFR subchapter I, inspected under 46 CFR, subchapters D or O, or certain dangerous cargoes.

Table 4 presents the affected population of U.S.-flagged vessels, facilities, and OCS facilities of this proposed rule.[68] For the vessel population, the Coast Guard assumes the same number of vessels that leave and enter service. Therefore, we assume the population to be constant over the 10-year period of analysis. We also make the same assumption for facilities and OCS facilities. Additionally, we assume that changes in the ownership of vessels and facilities would be very rare and any audits that would result from a change in ownership would be accounted for by the annual audit requirements. We request public comments on these assumptions, and generally, on the affected population.

Table 4: Estimated Affected U.S. Population of the Proposed Rule

Population Group	Total Number of Vessels or Facilities
Vessels	
U.S. towing vessels greater than 8 meters (26 feet) in registered length inspected under 46 CFR subchapter M that are engaged in towing a barge or barges inspected under 46 CFR subchapters D and O.	3,921
U.S. tankships inspected under 46 CFR subchapters D and O.	88
Self-propelled U.S. cargo and miscellaneous vessels—self-propelled vessels greater than 100 gross register tons inspected under 46 CFR subchapter I, except for commercial fishing vessels inspected under 46 CFR part 105.	574
Small U.S. passenger vessels carrying more than 12 passengers, including at least 1	50

[68] This data was retrieved from the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database in September 2022.

passenger-for-hire, that are engaged on international voyages.	
Small U.S. passenger vessels inspected under 46 CFR subchapter K (certificated to carry more than 150 passengers).	379
Large U.S. passenger vessels inspected under 46 CFR subchapter H.	34
OSVs inspected under 46 CFR subchapter L	426
U.S. MODUs subject to SOLAS Chapter XI-1 or Chapter XI-2 that are inspected under 46 CFR subchapter I-A.	1
U.S. barges inspected under 46 CFR subchapters D, O, or I (includes combination barges) carrying certain dangerous cargo in bulk or barges engaged on international voyages.	4,813
Total U.S.-flagged vessel population	**10,286 (1,775 owners and operators)**
Facilities	
Total facilities and OCS facilities (includes MTSA-regulated facilities)	**3,411 (1,708 owners and operators)**

Cost Analysis of the Proposed Rule

This proposed rule would impose costs on the U.S. maritime industry for cybersecurity requirements that include:

- Developing a Cybersecurity Plan, which includes designating a CySO, in proposed 33 CFR 101.630;
- Performing drills and exercises in proposed 33 CFR 101.635; and
- Ensuring and implementing cybersecurity measures in proposed 33 CFR 101.650, such as account security measures, device security measures, data security measures, cybersecurity training for personnel, training for reporting an incident, risk management, supply chain management, resilience, network segmentation, and physical security.

We present the costs associated with some of the regulatory provisions in the

following analysis; however, we are not able to estimate the costs fully for certain provisions because of the lack of data and the uncertainty associated with these provisions. Also, some regulatory provisions may be included in developing the Cybersecurity Plan and maintaining it on an annual basis; therefore, we may not have estimated a cost for these specific provisions in this analysis. We clarify this in the analysis where applicable and request public comment regarding these analyses.

In addition, U.S. barges inspected under 46 CFR, subchapters D, O, or I (including combination barges), carrying certain dangerous cargo in bulk or barges engaged on international voyages, represent a special case in our analysis of cybersecurity-related costs. Unlike other vessels in the affected population of this NPRM, in most cases, barges do not have IT or OT systems onboard. Many types of barges rely on the IT and OT systems onboard their associated towing vessels or the facilities where they deliver their cargo. This also means that barges are typically unmanned, making the costs associated with provisions such as cybersecurity training difficult to estimate. While we acknowledge that there are some barges with IT or OT systems onboard, for the purposes of this analysis, we calculate costs only for the affected population of barges related to developing, resubmitting, maintaining, and auditing the Cybersecurity Plan, as well as developing cybersecurity-related drill and exercise components.

We believe that the hour-burden estimates associated with the components of the Cybersecurity Plan should still be sufficient to capture the implementation of any cybersecurity measures identified as necessary by the owner or operator of a barge. In addition, we believe it should capture any burden associated with requests for waivers or equivalents for provisions that would not apply to a vessel or vessel company lacking significant IT or OT systems. The Coast Guard requests comment on our assumptions and cost estimates related to barges and their cybersecurity activities.

Cybersecurity Plan Costs

Each owner and operator of a U.S.-flagged vessel, facility, or OCS facility would be required to develop and submit a Cybersecurity Plan to the Coast Guard. The CySO would develop, implement, and verify a Cybersecurity Plan for each U.S.-flagged vessel, facility, or OCS facility. The owner or operator would submit the Plan for approval to the cognizant COTP or the OCMI for a facility or OCS facility, or to the MSC for a U.S.-flagged vessel. The contents of the Cybersecurity Plan are detailed in proposed § 101.630.

Unless otherwise stated, we used information and obtained estimates in this RIA from subject matter experts (SMEs) in the Coast Guard's offices of Design and Engineering Standards (CG-ENG), Commercial Vessel Compliance (CG-CVC), and Port and Facility Compliance (CG-FAC). We also obtained information from the U.S. Coast Guard Cyber Command (CGCYBER) and the National Maritime Security Advisory Committee (NMSAC).

The Coast Guard acknowledges that some owners and operators of medium-sized and larger facilities, OCS facilities, and U.S.-flagged vessels may have already adopted a cybersecurity posture and implemented measures to counter and prevent a cyber incident. We also acknowledge that owners and operators of smaller facilities, OCS facilities, and U.S.-flagged vessels may not have any cybersecurity measures in place. For the purpose of this analysis, we assume that all owners or operators of facilities, OCS facilities, and U.S.-flagged vessels would be required to comply with the full extent of the requirements of this proposed rule. However, we have survey data indicating that a portion of owners and operators of affected facilities and OCS facilities already have some cybersecurity measures in place.[69] We present this survey data in the applicable sections of the cost

[69] Readers can access the survey at https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html; accessed July 19, 2023.

analysis. For other regulatory provisions, we do not estimate regulatory costs for industry because the Coast Guard does not have data on the extent of cybersecurity measures currently in the industry for these provisions. The Coast Guard requests owners and operators of facilities, OCS facilities, and U.S.-flagged vessels who have some or most of the required cybersecurity processes and procedures in their current operations to provide comments on the outlining processes and procedures they have implemented.

We list the regulatory provisions included in developing and maintaining a Cybersecurity Plan that we did not estimate costs for in other sections of this RIA:

- Device security measures in § 101.650(b)(1) through (4);
- Supply chain management in § 101.650(f)(1) through (3);
- Cybersecurity Assessment in § 101.650(e)(1);
- Documentation of penetration testing results and identified vulnerabilities in § 101.650(e)(2);
- Routine system maintenance measures in § 101.650(e)(3)(i) through (v); and
- Development and maintenance of a Cyber Incident Response Plan in § 101.650(g)(2).

Developing a Cybersecurity Plan has five cost components: the initial development of the Plan; annual maintenance of the Plan (including amendments); revision and resubmission of the Plan as needed; renewal of the Plan after 5 years; and the cost for annual audits. Owners and operators of U.S.-flagged vessels, facilities, and OCS facilities would be required to submit their Cybersecurity Plan to the Coast Guard during the second annual audit of the currently approved VSP, FSP, or OCS FSP following the effective date of this proposed rule; therefore, submitting a Cybersecurity Plan for approval would likely not occur until the second year of the 10-year period of analysis.

The CySO would be responsible for all aspects of developing and maintaining the

Cybersecurity Plan. The Coast Guard does not have data on whether owners and operators of facilities, OCS facilities, and vessels would hire a dedicated, salaried employee to serve as a CySO. Proposed § 101.625 states that a CySO may perform other duties within an owner or operator's organization, and that a person may serve as a CySO for more than one U.S.-flagged vessel, facility, or OCS facility. For facilities and OCS facilities, this person may be the Facility Security Officer. For vessels, this person may be the Vessel Security Officer. When considering assigning the CySO role to the existing security officer, the owner or operator should consider the depth and scope of these new responsibilities in addition to existing security duties. For the purpose of this analysis, we assume that an existing person in a facility, OCS facility, or U.S.-flagged vessel company or organization would assume the duties and responsibilities of a CySO, and that owners and operators would not have to hire an individual to fill this position. This means that any costs associated with obtaining security credentials (including a Transportation Worker Identification Card) would already be incurred prior to the implementation of this proposed rule. Additionally, in the event that the designated CySO has security responsibilities that overlap with an existing Vessel, Facility, or Company Security Officer, we assume that those individuals will work together to handle those duties.

We use the Bureau of Labor Statistics' (BLS) "National Occupational Employment and Wage Estimates" for the United States for May 2022. A CySO would be comparable to the occupational category of "Information Security Analysts" according to BLS's labor categories with an occupational code of 15-1212 and an unloaded mean hourly wage rate of $57.63.[70] In order to obtain a loaded mean hourly wage rate, we use BLS's "Employer Costs for Employee Compensation" database to calculate the load

[70] Readers can access BLS's website at https://www.bls.gov/oes/2022/may/oes151212.htm to obtain information about the wage we used in this analysis; accessed May 5, 2023.

factor, which we applied to the unloaded mean hourly wage rate using fourth quarter data from 2022.[71] We determine the load factor for this occupational category to be about 1.46, rounded. We then multiply this load factor by the unloaded mean hourly wage rate of $57.63 to obtain a loaded mean hourly wage rate of about $84.14, rounded ($57.63 × 1.46).

Cybersecurity Plan Cost for Facilities and OCS Facilities

This proposed rule would require owners and operators of facilities and OCS facilities to create a Cybersecurity Plan for each facility within a company. For the purpose of this analysis, the cost to develop a Cybersecurity Plan is a function of the number of facilities, not the number of owners and operators, because an owner or operator may own more than one facility. Based on data obtained from the Coast Guard's Marine Information for Safety and Law Enforcement (MISLE) database, we estimate this NPRM would affect about 3,411 facilities and OCS facilities (including MTSA-regulated facilities), and about 1,708 owners and operators of these facilities. MISLE data contains incomplete information on owners and operators for 748 of the 3,411 facilities and OCS facilities included in the affected population. Of the 2,663 facilities and OCS facilities with complete information for owners and operators, we found 1,334 unique owners. This means that, on average, each owner owns

[71] A loaded mean hourly wage rate is what a company pays per hour to employ a person, not the hourly wage an employee receives. The loaded mean hourly wage rate includes the cost of non-wage benefits (health insurance, vacation, etc.). We calculated the load factor by accessing BLS's website at https://www.bls.gov/ and selecting the topic "Subjects" from the menu on this webpage. From the categories listed on this page, under the category titled "Pay and Benefits," we then selected the category of "Employment Costs." The next page is titled "Employment Cost Trends;" in the left margin, we selected the category "ECT Databases" at https://www.bls.gov/ncs/ect/data.htm. At this page, we selected the database titled "Employer Costs for Employee Compensation" using the "Multi-Screen" feature at https://data.bls.gov/cgi-bin/dsrv?cm. We then selected the category of "Private Industry Workers" at screen 1. At screen 2, we first selected the category "Total Compensation," then we continued to select "Transportation and Materials Moving Occupations" at screen 3, then "All Workers" at screens 4 and 5, and then for "Area," we selected "United States" at screen 6. At screen 7, we selected the category "Employer Cost for Employee Compensation." At screen 8, we selected the category "not seasonally adjusted." At screen 9, we selected the series ID, CMU2010000520000D. We used the "Cost of Compensation" for quarter 4 of 2022, or $33.07. We performed this process again to obtain the value for "Wages and Salaries," which we selected on screen 2. On screen 9, we selected the series ID CMU2020000520000D and obtained a value of $22.64. We divided $33.07 by $22.64 and obtained a load factor of 1.46, rounded; accessed May 3, 2023.

approximately 2 facilities (2,663 ÷ 1,334 = 2.0, rounded). We apply this rate of ownership to the remaining facilities and OCS facilities without complete ownership information to arrive at our total of 1,708 owners [1,334 + (748 ÷ 2)].

We use hour-burden estimates from Coast Guard SMEs and the currently approved OMB Information Collection Request (ICR), Control Number 1625-0077, titled, "Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and other Security-Related Requirements." The hour-burden estimates are 100 hours for developing the Cybersecurity Plan (average hour burden), 10 hours for annual maintenance of the Cybersecurity Plan (which would include amendments), 15 hours to resubmit Cybersecurity Plans every 5 years, and 40 hours to conduct annual audits of Cybersecurity Plans.

While the Cybersecurity Plan can be incorporated into an existing FSP for a facility or OCS facility, this does not mean that the Cybersecurity Plan is expected to be less complex to develop or maintain than an FSP. In general, the provisions outlined in this proposed rule are meant to reflect the depth and scope of the physical security provisions established by MTSA. As a result, we feel the hour-burden estimates for developing and maintaining the FSP represents a fair proxy for what is expected with respect to a Cybersecurity Plan. Nevertheless, the Coast Guard requests comment on the accuracy of these hour-burden estimates as they relate to developing a Cybersecurity Plan.

Based on estimates from the Coast Guard's FSP reviewers at local inspections offices, approximately 10 percent of Plans would need to be revised and resubmitted in the second year, which is consistent with the current resubmission rate for FSPs. Plans must be renewed after 5 years (occurring in the seventh year of the analysis period), and we estimate that 10 percent of renewals would also require revision and resubmission. We estimate the time to revise and resubmit the Cybersecurity Plan to be about half the

time to develop the Plan itself, or 50 hours in the second year of submission, and 7.5 hours after 5 years (in the seventh year of the analysis period).

Because we include the annual Cybersecurity Assessment in the cost to develop Cybersecurity Plans, and we do not assume that owners and operators will wait until the second year of analysis to begin developing the Plan or implementing related cybersecurity measures, we divide the estimated 100 hours to develop Plans equally across the first and second years of analysis. We estimate the first- and second-year (the first year of Plan submission) undiscounted cost to develop a Cybersecurity Plan for owners and operators of U.S. facilities and OCS facilities to be about $28,700,154 (3,411 Plans × 100 hours × $84.14). We estimate the second-year undiscounted cost for owners and operators to resubmit Plans for facilities or OCS facilities (or to send amendments) for corrections to be about $1,434,587 (341 Plans or amendments × 50 hours × $84.14). Therefore, we estimate the total undiscounted first- and second-year cost to facility and OCS facility owners and operators to develop, submit, and resubmit a Cybersecurity Plan to be approximately $30,134,741 ($28,700,154 + $1,434,587)).

In years 3 through 6 and years 8 through 10 of the analysis period, owners and operators of U.S. facilities and OCS facilities would be required to maintain their Cybersecurity Plans. This may include recordkeeping and documenting cybersecurity items at a facility or OCS facility, as well as amending the Plan. The CySO would be required to maintain each Plan for each facility or OCS facility. Maintaining the Plan does not occur in the second year (initial year of Plan submission) or in the renewal year, year 7 of the analysis period. We again obtain the hour-burden estimate for the annual maintenance of Plans from ICR 1625-0077, which is 10 hours.

In the same years of the analysis period, this proposed rule would also require owners and operators of facilities and OCS facilities to conduct annual audits. The audits would be necessary for owners and operators of facilities and OCS facilities to identify

vulnerabilities (via the Cybersecurity Assessment) and to mitigate them.[72] Audits would also be necessary if there is a change in the ownership of a facility, but because the costs for audits are estimated annually, this should capture audits as a result of very rare changes in ownership each year as well. The CySO would be responsible for ensuring the audit of a Cybersecurity Plan. Based on input provided by Coast Guard SMEs who review Plans at the Coast Guard, we estimate the time to conduct an audit to be about 40 hours for each Plan. We estimate the undiscounted cost for the annual maintenance of Cybersecurity Plans for facility and OCS facility owners and operators to be approximately $2,870,015 (3,411 facility Plans × 10 hours × $84.14). We estimate the undiscounted cost for annual audits of Cybersecurity Plans to be approximately $11,480,062 (3,411 facility Plans × 40 hours × $84.14). We estimate the total undiscounted annual cost each year in years 3 through 6 and 8 through 10 for Cybersecurity Plans to be approximately $14,350,077 ($2,870,015 + $11,480,062).

Because a Cybersecurity Plan approved by the Coast Guard is valid for 5 years, in year 7 of the analysis period, owners and operators of facilities and OCS facilities would be required to renew the approval of their Plans with the Coast Guard. We use the hour-burden estimate in ICR 1625-0077for renewing the Plan, which is 15 hours. The hour-burden estimate for revision and resubmission of renewals is half of the original hour-burden for renewals, or 7.5 hours. The CySO would be responsible for resubmitting the Cybersecurity Plan to the Coast Guard for renewal, including additional resubmissions because of corrections. We estimate the undiscounted cost for renewing and resubmitting a Cybersecurity Plan due to corrections to be approximately $4,520,211 [(3,411 facility Plans × 15 hours × $84.14) + (341 resubmitted facility Plans× 7.5 hours × $84.14)].

[72] The Jones Walker survey (see footnote 69) reports about 72 percent of ports and terminals conduct a risk assessment at least once a year. We did not estimate a separate cost for this item because the Coast Guard believes that a risk assessment can be a part of an annual audit. Readers can access the survey at https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html; accessed July 19, 2023.

We estimate the total discounted cost of this proposed rule for developing Cybersecurity Plans for facility and OCS facility owners and operators to be approximately $95,920,412 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $13,656,909, using a 7-percent discount rate. See table 5.

Table 5: Estimated Cost of the Proposed Rule for Facility and OCS Facility Cybersecurity Plans (2022 Dollars, 10-year Period of Analysis, 7- and 3-percent Discount Rates)

Year	Number of Companies (a)	Number of Submissions (b)	Number of Resubmissions (c)	CySO Wage (d)	Development Hours (e)	Annual Maintenance Hours (f)	Resubmission Hours (g)	Audit Hours (h)	Total Cost = [(b × d × (e + f + h)) + (c × d × g)]	7 Percent	3 Percent
1	1708	3411	0	$84.14	50	0	0	0	$14,350,077	$13,411,287	$13,932,114
2	1708	3411	341	$84.14	50	0	50	0	$15,784,664	$13,786,937	$14,878,560
3	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$11,713,937	$13,132,353
4	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$10,947,605	$12,749,858
5	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$10,231,407	$12,378,502
6	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$9,562,062	$12,017,964
7	1708	3411	341	$84.14	15	0	7.5	0	$4,520,211	$2,814,960	$3,675,345
8	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$8,351,875	$11,328,083
9	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$7,805,491	$10,998,139
10	1708	3411	0	$84.14	0	10	0	40	$14,350,077	$7,294,851	$10,677,805
Total									**$135,105,491**	**$95,920,412**	**$115,768,723**
Annualized									**$13,510,549**	**$13,656,909**	**$13,571,626**

Note: Totals may not sum due to independent rounding.

Cybersecurity Plan Cost for U.S.-Flagged Vessels

The methodology for owners and operators of U.S.-flagged vessels to develop a Cybersecurity Plan is the same as for U.S. facilities and OCS facilities. We estimate the affected vessel population to be about 10,286. We estimate the number of owners and operators of these vessels to be about 1,775.

We use estimates provided by Coast Guard SMEs and ICR 1625-0077 for the hour-burden estimates for vessels as we did for facilities and OCS facilities. The hour-burden estimates are 80 hours for developing the Cybersecurity Plan, 8 hours for annual Plan maintenance, 12 hours to renew the Plan every 5 years, and 40 hours to conduct annual audits of Plans for vessels. Similar to facilities, 10 percent of all Cybersecurity Plans for vessels would need to be resubmitted for corrections in the second year (initial year of Plan submission), and 10 percent of Cybersecurity Plans for vessels would need to be revised and resubmitted in the seventh year of the analysis period. Based on information from Coast Guard SMEs, we estimate the time to make corrections to the Plan in the second year would be about half of the initial time to develop the Plan, or 40 hours in the second year, and 6 hours in the seventh year. We include the annual Cybersecurity Assessment in the cost to develop Plans, and we do not assume that owners and operators will wait until the second year of analysis to begin developing the Cybersecurity Plan or implementing related cybersecurity measures. Therefore, we divide the estimated 80 hours to develop Plans equally across the first and second years of analysis.

The methodology to determine the cost to develop a Cybersecurity Plan for U.S.-flagged vessels is slightly different than the methodology for facilities and OCS facilities. The Coast Guard does not believe that a CySO for U.S.-flagged vessels would expend 80 hours developing a Plan for each vessel in a company's fleet. For example, if a vessel owner or operator has 10 vessels, it would take a CySO 800 hours of time to develop

Plans for all 10 vessels, which is nearly 40 percent of the total hours of work in a calendar year. It is more likely that the CySO would create a master Cybersecurity Plan for all the vessels in the fleet, and then tailor each Plan according to a specific vessel, as necessary.

Because a large portion of the provisions required under this proposed rule would impact company-wide policies regarding network, account, and data security practices, as well as company-wide cybersecurity training, reporting procedures, and testing, we do not believe there will be much variation in how these provisions are implemented between specific vessels owned by the same owner or operator. Therefore, the cost to develop a Cybersecurity Plan for vessels becomes a function of the number of vessel owners and operators and not a function of the number of vessels.

When a vessel owner or operator submits a Plan to the Coast Guard for approval, the owner or operator would send the master Cybersecurity Plan, which might include a more tailored or abbreviated Plan for each vessel. For example, the owner or operator of 10 vessels would send the master Cybersecurity Plan along with the tailored Plans for each vessel in one submission to the Coast Guard for approval, instead of 10 separate documents. The Coast Guard requests comments on these assumptions related to master and tailored vessel Cybersecurity Plans.

We estimate the first- and second-year (initial year of Plan submission) undiscounted cost for owners and operators of U.S.-flagged vessels to develop a Cybersecurity Plan to be approximately $11,947,880 (1,775 Plans × 80 hours × $84.14) split over the first two years of analysis. We estimate the second-year undiscounted cost for owners and operators to resubmit vessel Plans (or send amendments) for corrections to be approximately $599,077 (178 Plans or amendments × 40 hours × $84.14). Therefore, we estimate the total undiscounted first- and second-year cost to the owners and operators of U.S.-flagged vessels to develop a Cybersecurity Plan to be

approximately $12,546,957 ($11,947,880 + $599,077).

As with facilities and OCS facilities, in years 3 through 6 and years 8 through 10 of the analysis period, CySOs, on behalf of owners and operators of U.S.-flagged vessels, would be required to maintain their Cybersecurity Plans. We again obtain the hour-burden estimate for annual maintenance of Plans from ICR 1625-0077, which is 8 hours. In the same years of the analysis period, this proposed rule would also require owners and operators of U.S.-flagged vessels to conduct annual audits. The audits would be necessary for owners and operators of U.S.-flagged vessels to identify vulnerabilities through the Cybersecurity Assessment and to mitigate them. Audits would also be necessary if there is a change in the ownership of a vessel. The CySO would likely conduct an audit of the master Cybersecurity Plan, which would include each vessel, instead of conducting a separate audit for each individual vessel.

The time estimate for a CySO to conduct an audit for U.S.-flagged vessels in a fleet is the same as it is for facilities and OCS facilities, or 40 hours per Plan. We estimate the undiscounted cost for the annual maintenance of Cybersecurity Plans for the owners and operators of U.S.-flagged vessels to be about $1,194,788 (1,775 Plans × 8 hours × $84.14). We estimate the undiscounted cost for annual audits of Cybersecurity Plans to be approximately $5,973,940 (1,775 Plans × 40 hours × $84.14). We estimate the total undiscounted annual cost each year in years 3 through 6 and 8 through 10 for Cybersecurity Plans to be approximately $7,168,728 ($1,194,788 + $5,973,940).

Again, as with facilities and OCS facilities, Coast Guard approval for the Cybersecurity Plan is valid for 5 years. Therefore, in year 7 of the analysis period, owners and operators of U.S.-flagged vessels would be required to renew their Plans with the Coast Guard. We use the hour-burden estimate in ICR 1625-0077 for Plan renewal, which is 12 hours. The CySO would be responsible for resubmitting the Cybersecurity Plan to the Coast Guard for renewal. We estimate the undiscounted cost for owners and

operators of U.S.-flagged vessels to renew the Plan to be approximately $1,882,044 [(1,775 Plans × 12 hours × $84.14) + (178 resubmitted vessel Plans × 6 hours × $84.14)].

We estimate the total discounted cost of this proposed rule for owners and operators of U.S.-flagged vessels to develop Cybersecurity Plans to be approximately $45,420,922 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $6,466,917, using a 7-percent discount rate. See table 6.

Table 6: Estimated Cost of the Proposed Rule for U.S.-Flagged Vessel Cybersecurity Master Plan Development (2022 Dollars, 10-year Period of Analysis, 7- and 3-percent Discount Rates)

Year	Number of Companies (a)	Number of Submissions (b)	Number of Resubmissions (c)	CySO Wage (d)	Development Hours (e)	Annual Maintenance Hours (f)	Resubmission Hours (g)	Audit Hours (h)	Total Cost = [(b × d × (e + f + h)) + (c × d × g)]	7 Percent	3 Percent
1	1775	1775	0	$84.14	40	0	0	0	$5,973,940	$5,583,121	$5,799,942
2	1775	1775	178	$84.14	40	0	40	0	$6,573,017	$5,741,128	$6,195,699
3	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$5,851,817	$6,560,402
4	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$5,468,988	$6,369,322
5	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$5,111,204	$6,183,808
6	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$4,776,826	$6,003,697
7	1775	1775	178	$84.14	12	0	6	0	$1,882,044	$1,172,042	$1,530,274
8	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$4,172,265	$5,659,060
9	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$3,899,313	$5,494,233
10	1775	1775	0	$84.14	0	8	0	40	$7,168,728	$3,644,218	$5,334,207
Total									$64,610,097	**$45,420,922**	**$55,130,644**
Annualized									$6,461,010	**$6,466,917**	**$6,462,993**

Note: Totals may not sum due to independent rounding.

Drills

In proposed § 101.635(b), this NPRM would require drills that test the proficiency of U.S.-flagged vessel, facility, and OCS facility personnel who have assigned cybersecurity duties. The drills would enable the CySO to identify any cybersecurity deficiencies that need to be addressed. The CySO would need to conduct the drills every 3 months or quarterly, (which is consistent with the MTSA regulations for drills for vessels, facilities, and OCS facilities in 33 CFR parts 104, 105 and 106, respectively), and they may be held in conjunction with other security or non-security-related drills, as appropriate. The drills would test individual elements of the Plan, including responses to cybersecurity threats and incidents.

The Coast Guard does not have data on who is currently conducting cybersecurity drills in either the population of facilities and OCS facilities or the population of U.S.-flagged vessels. Therefore, we assume that the entire population of facilities and U.S.-flagged vessels would need to develop new cybersecurity related drills to comply with the proposed requirements. However, because the affected populations are already required to conduct drills in accordance with 33 CFR parts 104, 105, and 106, and the proposed rule allows for owners and operators to hold cybersecurity drills in conjunction with other security and non-security related drills, we assume that owners and operators will hold these new drills in conjunction with existing drills and will not require additional time from participants. This means that the only new cost associated with the proposed cybersecurity drills is the development of cybersecurity components to add to existing drills. Coast Guard SMEs who are familiar with MTSA's requirements and practices for drills and exercises estimate that it would take a CySO 0.5 hours (30 minutes) to develop new cybersecurity components to add to existing drills. This time estimate is based on the expected ease with which a CySO can access widely available resources and planning materials for developing cybersecurity drills online. The Coast

Guard requests the public to comment on the accuracy of our estimates related to the development of cybersecurity drill components.

The CySO would be the person who develops cybersecurity components to add to existing drills. Each CySO, on behalf of the owner or operator of a facility or OCS facility, would be required to develop the drill's components beginning in the first year of the analysis period and document procedures in the Cybersecurity Plan.

Using the number of facilities owners and operators we presented earlier—or 1,708—the CySO's loaded mean hourly wage rate, the estimated time to develop the drill's components or 0.5 hours (30 minutes), and the frequency of the drill, or every 3 months, we estimate the cost for facilities to develop cybersecurity components for drills. We estimate the undiscounted annual cost of drills for facility and OCS facility owners and operators to be approximately $287,422 (1,708 facility CySOs × 4 drills per year × 0.5 hours per drill × $84.14. We estimate the total discounted cost of drills for owners and operators of facilities and OCS facilities to be approximately $2,018,733 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $287,422, using a 7-percent discount rate. See table 7.

Table 7: Estimated Drill Costs of the Proposed Rule for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Facility Companies	CySO Wage	Drill Development Hours	Frequency of Drills	Total Cost	7 Percent	3 Percent
1	1708	$84.14	0.5	4	$287,422	$268,619	$279,050
2	1708	$84.14	0.5	4	$287,422	$251,046	$270,923
3	1708	$84.14	0.5	4	$287,422	$234,622	$263,032
4	1708	$84.14	0.5	4	$287,422	$219,273	$255,371
5	1708	$84.14	0.5	4	$287,422	$204,928	$247,933
6	1708	$84.14	0.5	4	$287,422	$191,521	$240,711
7	1708	$84.14	0.5	4	$287,422	$178,992	$233,700
8	1708	$84.14	0.5	4	$287,422	$167,282	$226,894
9	1708	$84.14	0.5	4	$287,422	$156,339	$220,285
10	1708	$84.14	0.5	4	$287,422	$146,111	$213,869
Total					$2,874,220	**$2,018,733**	**$2,451,768**
Annualized						**$287,422**	**$287,422**

Note: Totals may not sum due to independent rounding.

We use the same methodology and estimates for U.S.-flagged vessel drills. As we presented previously, there are about 1,775 CySOs, on behalf of owners and operators of U.S.-flagged vessels, who would be required to develop drills with this proposed rule. We estimate the undiscounted annual cost of drills for the owners and operators of U.S.-flagged vessels to be approximately $298,697 (1,775 vessel CySOs × 4 drills per year × 0.5 hours per drill × $84.14). We estimate the total discounted cost of drills for U.S.-flagged vessels to be approximately $2,097,922 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $298,697, using a 7-percent discount rate. See table 8.

Table 8: Estimated Drill Costs of the Proposed Rule for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Vessel Companies	CySO Wage	Drill Development Hours	Frequency of Drills	Total Cost	7 Percent	3 Percent
1	1775	$84.14	0.5	4	$298,697	$279,156	$289,997
2	1775	$84.14	0.5	4	$298,697	$260,894	$281,551
3	1775	$84.14	0.5	4	$298,697	$243,826	$273,350
4	1775	$84.14	0.5	4	$298,697	$227,875	$265,388
5	1775	$84.14	0.5	4	$298,697	$212,967	$257,659
6	1775	$84.14	0.5	4	$298,697	$199,034	$250,154
7	1775	$84.14	0.5	4	$298,697	$186,013	$242,868
8	1775	$84.14	0.5	4	$298,697	$173,844	$235,794
9	1775	$84.14	0.5	4	$298,697	$162,471	$228,926
10	1775	$84.14	0.5	4	$298,697	$151,842	$222,259
Total					$2,986,970	**$2,097,922**	**$2,547,946**
Annualized						**$298,697**	**$298,697**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of this proposed rule for drills for the owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to be approximately $4,116,655 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $586,119, using a 7-percent discount rate. See table 9.

Table 9: Estimated Costs of the Proposed Rule for Drills (Facilities, OCS Facilities, and U.S.-Flagged Vessels) (2022 Dollars, 10-year period of Analysis, 7- and 3-percent Discount Rates)

Year	Facilities Drill Cost	Vessel Drill Cost	Total Cost	7 Percent	3 Percent
1	$287,422	$298,697	$586,119	$547,775	$569,048
2	$287,422	$298,697	$586,119	$511,939	$552,473
3	$287,422	$298,697	$586,119	$478,448	$536,382
4	$287,422	$298,697	$586,119	$447,147	$520,759
5	$287,422	$298,697	$586,119	$417,895	$505,591
6	$287,422	$298,697	$586,119	$390,556	$490,865
7	$287,422	$298,697	$586,119	$365,005	$476,568
8	$287,422	$298,697	$586,119	$341,127	$462,688
9	$287,422	$298,697	$586,119	$318,810	$449,211
10	$287,422	$298,697	$586,119	$297,953	$436,128
Total	$2,874,220	$2,986,970	$5,861,190	**$4,116,655**	**$4,999,713**
Annualized				**$586,119**	**$586,119**

Note: Totals may not sum due to independent rounding.

Exercises

In proposed § 101.635(c), this NPRM would require exercises that test the communication and notification procedures of U.S.-flagged vessels, facilities, and OCS facilities. These exercises may be vessel- or facility-specific, or part of a cooperative exercise program or comprehensive port exercises. The exercises would be a full test of the cybersecurity program with active participation by the CySO and may include Government authorities and vessels visiting a facility. The exercises would have to be conducted at least once each calendar year, with no more than 18 months between exercises. As with drills, we assume that exercises will begin in the first year of the analysis period as CySOs develop Cybersecurity Plans. We also assume that the exercises developed to satisfy § 101.635(c) would also satisfy the exercise requirements outlined in § 101.650 (g)(2) and (3), which requires the exercise of the Cybersecurity Plan and Cyber Incident Response Plan.

The Coast Guard does not have data on who is currently conducting cybersecurity exercises in either the population of facilities and OCS facilities or the population of

U.S.-flagged vessels. Therefore, we assume that the entire populations would need to develop new cybersecurity-related exercises to comply with the proposed requirements. However, because the affected populations are already required to conduct exercises in accordance with 33 CFR parts 104, 105, and 106, and because this proposed rule allows for owners and operators to hold cybersecurity exercises in conjunction with other exercises, we assume that owners and operators will hold these new exercises in conjunction with existing exercises. This will not require any additional time from participants, which means that the only new cost associated with the proposed cybersecurity exercises is the development of cybersecurity components to add to existing exercises.

Coast Guard SMEs familiar with MTSA's requirements and practices for drills and exercises estimate that it would take a CySO 8 hours to develop new cybersecurity components to add to existing exercises. This time estimate is based on the expected ease with which a CySO can access widely available resources and planning materials for developing cybersecurity exercises online[73] and the proliferation of cybersecurity components already being added to AMSC exercises around the United States.[74] The Coast Guard requests comment on the accuracy of our estimates related to the development of cybersecurity exercise components.

We assume each CySO, on behalf of the owner and operator of a facility or OCS facility, would develop the exercises specified in the proposed rule. Using the 1,708 facility owners and operators we presented earlier, the CySO's loaded mean hourly wage rate, the 8-hour estimate for developing the exercise components, and one annual exercise, we estimate the cost for facilities to develop cybersecurity exercise components.

---

[73] For example, CISA offers free resources on cybersecurity scenarios and cybersecurity exercises on their website. See https://www.cisa.gov/cybersecurity-training-exercises, accessed July 19, 2023.

[74] See https://digitaleditions.walsworthprintgroup.com/publication/?i=459304&article_id=2956672&view=articleBrowser for just one example of AMSC cyber exercises in recent years; accessed July 19, 2023.

We estimate the undiscounted annual cost of exercises for owners and operators of facilities and OCS facilities to be approximately $1,149,689 (1,708 facility CySOs × 8 hours per exercise × $84.14). We estimate the total discounted cost of exercises for facility owners and operators to be about $8,074,935 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $1,149,689, using a 7-percent discount rate. See table 10.

Table 10: Estimated Exercise Costs of the Proposed Rule for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Facility Companies	CySO Wage	Exercise Development Hours	Exercises per Year	Total Cost	7 Percent	3 Percent
1	1708	$84.14	8	1	$1,149,689	$1,074,476	$1,116,203
2	1708	$84.14	8	1	$1,149,689	$1,004,183	$1,083,692
3	1708	$84.14	8	1	$1,149,689	$938,489	$1,052,128
4	1708	$84.14	8	1	$1,149,689	$877,092	$1,021,484
5	1708	$84.14	8	1	$1,149,689	$819,712	$991,732
6	1708	$84.14	8	1	$1,149,689	$766,086	$962,846
7	1708	$84.14	8	1	$1,149,689	$715,969	$934,802
8	1708	$84.14	8	1	$1,149,689	$669,129	$907,575
9	1708	$84.14	8	1	$1,149,689	$625,355	$881,141
10	1708	$84.14	8	1	$1,149,689	$584,444	$855,477
Total					$11,496,890	**$8,074,935**	**$9,807,080**
Annualized						**$1,149,689**	**$1,149,689**

Note: Totals may not sum due to independent rounding.

We use the same methodology and estimates for vessel exercises that we use for facilities. About 1,775 CySOs, on behalf of vessel owners and operators, would be required to conduct exercises with this proposed rule. We estimate the undiscounted annual cost of exercises for the owners and operators of U.S.-flagged vessels to be approximately $1,194,788 (1,775 vessel CySOs × 8 hours per exercise × $84.14). We estimate the total discounted cost of exercises for U.S.-flagged vessels to be approximately $8,391,691 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $1,194,788, using a 7-percent discount rate. See table 11.

Table 11: Estimated Drill Costs of the Proposed Rule for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Vessel Companies	CySO Wage	Exercise Development Hours	Exercises per Year	Total Cost	7 Percent	3 Percent
1	1775	$84.14	8	1	$1,194,788	$1,116,624	$1,159,988
2	1775	$84.14	8	1	$1,194,788	$1,043,574	$1,126,202
3	1775	$84.14	8	1	$1,194,788	$975,303	$1,093,400
4	1775	$84.14	8	1	$1,194,788	$911,498	$1,061,554
5	1775	$84.14	8	1	$1,194,788	$851,867	$1,030,635
6	1775	$84.14	8	1	$1,194,788	$796,138	$1,000,616
7	1775	$84.14	8	1	$1,194,788	$744,054	$971,472
8	1775	$84.14	8	1	$1,194,788	$695,377	$943,177
9	1775	$84.14	8	1	$1,194,788	$649,886	$915,706
10	1775	$84.14	8	1	$1,194,788	$607,370	$889,034
Total					**$11,947,880**	**$8,391,691**	**$10,191,784**
Annualized						**$1,194,788**	**$1,194,788**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of this proposed rule for the owners and operators of U.S. facilities, OCS facilities, and U.S.-flagged vessels for exercises to be approximately $16,466,625 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $2,344,477, using a 7-percent discount rate. See table 12.

Table 12: Estimated Cost of the Proposed Rule for Exercises (Facilities, OCS Facilities, and U.S.-Flagged Vessels) (2022 Dollars, 10-year Period of Analysis, 7- and 3-percent Discount Rates)

Year	Facilities Exercise Cost	Vessel Exercise Cost	Total Cost	7 Percent	3 Percent
1	$1,149,689	$1,194,788	$2,344,477	$2,191,100	$2,276,191
2	$1,149,689	$1,194,788	$2,344,477	$2,047,757	$2,209,894
3	$1,149,689	$1,194,788	$2,344,477	$1,913,792	$2,145,529
4	$1,149,689	$1,194,788	$2,344,477	$1,788,590	$2,083,037
5	$1,149,689	$1,194,788	$2,344,477	$1,671,580	$2,022,366
6	$1,149,689	$1,194,788	$2,344,477	$1,562,224	$1,963,463
7	$1,149,689	$1,194,788	$2,344,477	$1,460,022	$1,906,274
8	$1,149,689	$1,194,788	$2,344,477	$1,364,507	$1,850,752
9	$1,149,689	$1,194,788	$2,344,477	$1,275,240	$1,796,846
10	$1,149,689	$1,194,788	$2,344,477	$1,191,813	$1,744,511
Total	$11,496,890	$11,947,880	$23,444,770	**$16,466,625**	**$19,998,863**
Annualized				**$2,344,477**	**$2,344,477**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of this proposed rule for the owners and operators of facilities, OCS facilities, and U.S.-flagged vessels, to conduct annual drills and exercises to be approximately $20,583,281 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $2,930,596, using a 7-percent discount rate. See table 13.

Table 13: Summary of Drill and Exercise Discounted Costs of the Proposed Rule (2022 Dollars, 10-year Discounted Costs, 7-percent Discount Rate)

	Facilities and OCS Facilities	U.S.-flagged Vessels	Total Cost
Drills	$2,018,733	$2,097,922	**$4,116,655**
Exercises	$8,074,935	$8,391,691	**$16,466,626**
Total	$10,093,668	$10,489,613	**$20,583,281**
Annualized			**$2,930,596**

Note: Totals may not sum due to independent rounding.

Cybersecurity Measure Costs

The remaining regulatory provisions with associated costs are the cybersecurity measures in proposed § 101.650. There are five cost provisions associated with cybersecurity measures: account security measures; cybersecurity training for personnel; penetration testing; resilience; and risk management.

The first provision is account security measures in proposed § 101.650(a). The owners and operators of each U.S.-flagged vessel, facility, and OCS facility would ensure that account security measures are implemented and documented. This includes general account security measures in proposed § 101.650(a)(1) through (3) and (5) through (7) and multifactor authentication for end users in proposed § 101.650(a)(4). Based on the Jones Walker "Ports and Terminals Cybersecurity Survey," (see footnote 69), 87 percent of facilities currently have account security measures, and 83 percent of facilities currently use multifactor authentication software. Using the total number of 1,708 facility and OCS facility owners and operators, we multiply this number by 0.13 and 0.17, respectively, to obtain the number of facility owners and operators who would need to implement security measures and have multifactor authentication software under this

proposed rule, or about 222 and 290, respectively. The Coast Guard acknowledges that the survey data used here may lead us to underestimate the costs incurred by the population of facilities and OCS facilities, given the high rate of respondents who indicated that they have these measures in place. Accordingly, we request comments on the accuracy of these rates of implementation in the population of facilities and OCS facilities.

We obtain the hour estimates and the labor category for these security measures for implementing and managing account security from NMSAC members with extensive experience in contracting to implement similar account security measures for facilities and OCS facilities in the affected population. A Database Administrator would ensure that account security measures are implemented. Using wage data from BLS's Occupational Employment and Wage Statistics (OEWS) program as previously referenced, the unloaded mean hourly wage rate for this labor category, occupational code of 15-1242, is $49.29.[75] Using Employer Costs for Employee Compensation data from BLS, we apply the same load factor of 1.46 to the aforementioned wage rate to obtain a loaded mean hourly wage rate of approximately $71.96.

It would take a Database Administrator about 8 hours to implement the account security measures and 8 hours for account security management annually thereafter for 222 U.S. facility and OCS facility companies. We estimate the undiscounted initial-year cost to implement account security for 222 facilities and OCS facilities and the annually recurring cost of account security management to be approximately $127,801, rounded [(222 facilities × ($71.96 × 8 hours)].

The number of facility and OCS facility companies that would need multifactor authentication security is about 290. Based on estimates from CG-FAC SMEs with experience implementing multifactor authentication at other Government agencies,

[75] See https://www.bls.gov/oes/2022/may/oes151242.htm, accessed July 12, 2023.

implementation of multifactor authentication would cost each facility anywhere from $3,000 to $15,000 in the initial year for setup and configuration. For the purposes of this analysis, we use the average of approximately $9,000 for the costs of initial setup and configuration. It would also cost each facility approximately $150 per end user for annual maintenance and support of the implemented multifactor authentication system. These costs represent the average costs for implementing and maintaining a multifactor authentication system across different organization and company sizes based on the SMEs' experience.

We use the total number of estimated employees at an affected facility company in our analysis of costs because the Coast Guard currently lacks data on (1) which systems in use at a facility or OCS facility would need multifactor authentication, and (2) whether only a subset of the total employees would require access. This is largely because owners and operators have the discretion to designate both critical IT and OT systems as well as the number of employees needing access. Therefore, for the purpose of this analysis, we assume all employees would need multifactor authentication access. The Coast Guard requests comment on the accuracy of our cost estimates for implementing and maintaining multifactor authentication, and if only select systems or certain employees would require multifactor authentication access in most cases.

We obtain the average number of facility employees from a Coast Guard contract that uses D&B Hoovers' database for company employee data (available in the docket for this rulemaking, see the **Public Participation and Request for Comments** section of this preamble.) The average number of employees at a facility company is 74. We estimate the undiscounted initial-year cost to implement multifactor authentication for 290 facility and OCS facility companies to be approximately $2,610,000 (290 facilities × $9,000). We estimate the undiscounted initial-year and annual cost for multifactor authentication support and maintenance at facilities and OCS facilities to be

approximately $3,219,000 (290 facility companies × 74 employees × $150).

We estimate the total undiscounted initial-year cost to implement account security measures for facilities and OCS facilities to be approximately $5,956,801 ($127,801 cost to implement account security measures + $2,610,000 cost to set up and configure multifactor authentication + $3,219,000 cost for multifactor authentication support). We estimate the undiscounted annual cost in years 2 through 10 to be approximately $3,346,801 ($127,801 cost to manage account security + $3,219,000 cost to maintain and provide multifactor authentication support).

We estimate the total discounted cost to implement account security measures for (1) 222 facilities and OCS facilities that would need to implement general account security measures and (2) 290 facilities and OCS facilities that would need to implement multifactor authentication to be approximately $25,945,783 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $3,694,096, using a 7-percent discount rate. See table 14.

Table 14: Estimated Account Security Measure Costs of the Proposed Rule for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Account Security Management Costs	Multifactor Authentication Costs	Total Cost	7 Percent	3 Percent
1	$127,801	$5,829,000	$5,956,801	$5,567,104	$5,783,302
2	$127,801	$3,219,000	$3,346,801	$2,923,226	$3,154,681
3	$127,801	$3,219,000	$3,346,801	$2,731,987	$3,062,797
4	$127,801	$3,219,000	$3,346,801	$2,553,258	$2,973,589
5	$127,801	$3,219,000	$3,346,801	$2,386,223	$2,886,980
6	$127,801	$3,219,000	$3,346,801	$2,230,115	$2,802,893
7	$127,801	$3,219,000	$3,346,801	$2,084,219	$2,721,255
8	$127,801	$3,219,000	$3,346,801	$1,947,869	$2,641,996
9	$127,801	$3,219,000	$3,346,801	$1,820,438	$2,565,044
10	$127,801	$3,219,000	$3,346,801	$1,701,344	$2,490,334
Total			$36,078,010	**$25,945,783**	**$31,082,871**
Annualized			$3,607,801	**$3,694,096**	**$3,643,861**

Note: Totals may not sum due to independent rounding.

Owners and operators of U.S.-flagged vessels would need to implement the same

account security measures as facilities. The population of vessels affected, where applicable, would be about 5,473, rather than 10,286, because we subtract the barge population of 4,813 from 10,286, the total number of affected vessels. Because barges are unmanned, we assume they do not have computer systems onboard and, therefore, may not require account security measure implementation.

The number of affected vessel owners and operators would be about 1,602, excluding 173 barge owners and operators that do not own or operate other affected vessels. Based on the NMSAC estimates detailed above, it would take a Database Administrator about 8 hours to implement the account security measures and 8 hours to manage account security annually thereafter on behalf of each owner and operator of a vessel. We estimate the undiscounted initial-year cost to implement and annually recurring cost to manage account security measures for owners and operators of U.S.-flagged vessels, excluding barge owners and operators, to be approximately $922,239 [(1,602 vessel owners and operators × (8 hours × $71.96)].

The number of owners and operators who would require multifactor authentication security is about 1,602, for approximately 5,473 vessels. Based on Coast Guard information, multifactor authentication systems would be implemented at the company level because networks and account security policies would be managed at the company level, and not for each individual vessel. Any security updates or multifactor authentication programs implemented at the company level could be pushed out to devices located on board vessels owned or operated by the company. We use the same cost estimate from CG-FAC that we use for facilities. It would cost the owner or operator of a vessel approximately $9,000 to implement multifactor authentication in the first year and about $150 annually for multifactor authentication support and maintenance per end user. To determine the number of employees for each vessel company, we use data from the certificate of inspection manning requirements in MISLE for each vessel

subpopulation.[76] We assume 2 crews and multiply the total number of seafaring crew by 1.33 to account for shoreside staff in order to obtain an estimate of total company employees per vessel.[77] We estimate the total undiscounted initial-year cost to implement multifactor authentication for 1,602 vessel owners and operators to be approximately $14,418,000 (1,602 vessel owners and operators × $9,000).

To calculate the annual cost per end user, we multiply the number of vessels for a given vessel type by the average number of employees per vessel and the $150 annual cost of support and maintenance. For example, there are about 426 OSVs in the affected population, with an average number of 16 employees for each OSV. Therefore, the undiscounted annual cost of support and maintenance for OSV owners and operators would be approximately $1,022,400 (16 employees per each OSV (including shoreside) × $150 × 426 OSVs). We perform this calculation for each vessel type in the affected population and add the costs together to obtain the total initial-year cost and annual cost thereafter. We estimate the total undiscounted annual cost for multifactor authentication maintenance and support on vessels to be about $18,938,100 (number of employees for each vessel type × $150 × number of vessels for each vessel type). See table 15. We add these costs to the previously calculated implementation costs to obtain the initial-year costs associated with multifactor authentication of $33,356,100 ($14,418,000 implementation costs + $18,938,100 annual support and maintenance costs) as seen in column 3 of table 15.

Table 15: Estimated Annual Multifactor Authentication Support and Maintenance Costs of the Proposed Rule for U.S.-flagged Vessels Companies by Vessel Type (2022 Dollars)

[76] Manning requirements for U.S.-flagged vessels were established by regulation in 46 CFR part 15.
[77] To estimate the average number of mariners and shoreside employees for each company, Coast Guard conducted an internet search for publicly available employment data for the owners and operators of MTSA-regulated vessels. In total, Coast Guard was able to identify eight MTSA-regulated vessel owners and operators that publicly provided their shoreside and seafarer employment numbers. Using this data, we calculated the percentage of total employees working shoreside for each vessel. We then took an average of these percentages and applied that average to the population of MTSA vessel owners and operators. The percentage of shoreside employees ranged from 8 to 87 percent, with an average of 33 percent, which we used for each subpopulation of vessels.

Vessel Type	Number of Vessels	Number of Employees Per Vessel (Includes Shoreside)	Multifactor Authentication Annual Cost Per End User	Annual Costs
MODU	1	372	$150	$55,800
Subchapter I Vessels	574	82	$150	$7,060,200
OSVs	426	16	$150	$1,022,400
Subchapter H Passenger Vessels	34	85	$150	$433,500
Subchapter K Passenger Vessels	379	35	$150	$1,989,750
Subchapter M Towing Vessels	3921	13	$150	$7,645,950
Subchapter D and Combination Subchapters O&D Tank Vessels	88	40	$150	$528,000
Subchapters K and T International Passenger Vessels	50	27	$150	$202,500
Total				**$18,938,100**

Note: Totals may not sum due to independent rounding.

We estimate the total undiscounted initial-year cost to implement account security measures in proposed § 101.650(a)(1) through (3), and (5) through (7) and multifactor authentication for end users in proposed § 101.650(a)(4) for 1,602 U.S.-flagged vessels to be approximately $34,278,339 ($922,239 cost to implement account security + $33,356,100 cost to implement and provide multifactor support costs). We estimate the total undiscounted annual cost in years 2 through 10 to be approximately $19,860,339 ($922,239 cost to manage account security + $18,938,100 cost to maintain and provide multifactor authentication).

We estimate the total discounted cost to implement all the account security measures in proposed § 101.650(a)(1) through (3), and (5) through (7) and multifactor authentication for end users in proposed § 101.650(a)(4) for 1,602 U.S.-flagged vessels to be approximately $152,965,477 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $21,778,843 using a 7-percent discount rate. See table 16.

Table 16: Estimated Account Security Measure Costs of the Proposed Rule for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Account Security Management Costs	Multifactor Authentication Costs	Total Cost	7 Percent	3 Percent
1	$922,239	$33,356,100	$34,278,339	$32,035,831	$33,279,941
2	$922,239	$18,938,100	$19,860,339	$17,346,789	$18,720,274
3	$922,239	$18,938,100	$19,860,339	$16,211,953	$18,175,024
4	$922,239	$18,938,100	$19,860,339	$15,151,358	$17,645,654
5	$922,239	$18,938,100	$19,860,339	$14,160,147	$17,131,703
6	$922,239	$18,938,100	$19,860,339	$13,233,782	$16,632,721
7	$922,239	$18,938,100	$19,860,339	$12,368,021	$16,148,273
8	$922,239	$18,938,100	$19,860,339	$11,558,898	$15,677,935
9	$922,239	$18,938,100	$19,860,339	$10,802,709	$15,221,296
10	$922,239	$18,938,100	$19,860,339	$10,095,989	$14,777,957
Total			$213,021,390	**$152,965,477**	**$183,410,778**
Annualized			$21,302,139	**$21,778,843**	**$21,501,338**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost to implement account security measures for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities, including multifactor authentication, to be approximately $178,911,259 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $25,472,938, using a 7-percent discount rate. See table 17.

Table 17: Summary of Account Security Measure Costs of the Proposed Rule for Facilities, OCS Facilities, and U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rate)

Year	Facilities and OCS Facilities Cost	U.S.-flagged Vessels Cost	Total Cost	7 Percent	3 Percent
1	$5,956,801	$34,278,339	$40,235,140	$37,602,935	$39,063,243
2	$3,346,801	$19,860,339	$23,207,140	$20,270,015	$21,874,955
3	$3,346,801	$19,860,339	$23,207,140	$18,943,939	$21,237,821
4	$3,346,801	$19,860,339	$23,207,140	$17,704,616	$20,619,243
5	$3,346,801	$19,860,339	$23,207,140	$16,546,370	$20,018,683
6	$3,346,801	$19,860,339	$23,207,140	$15,463,897	$19,435,614
7	$3,346,801	$19,860,339	$23,207,140	$14,452,240	$18,869,529
8	$3,346,801	$19,860,339	$23,207,140	$13,506,767	$18,319,931
9	$3,346,801	$19,860,339	$23,207,140	$12,623,147	$17,786,340
10	$3,346,801	$19,860,339	$23,207,140	$11,797,333	$17,268,292

Total			**$249,099,400**	**$178,911,259**	**$214,493,651**
Annualized			**$24,909,940**	**$25,472,938**	**$25,145,199**

Note: Totals may not sum due to independent rounding.

Cybersecurity Training Cost

The second cost provision under cybersecurity measures, in proposed § 101.650(d), would be training. All persons with access to IT and OT would need annual training in topics such as the relevant aspects of the owner or operator's specific cybersecurity technology and concerns, recognition of threats and incidents, and incident reporting procedures. Given the importance of having a workforce trained on onsite cybersecurity systems as soon as possible to detect and mitigate cyber incidents, cybersecurity training would be verified during annual inspections following the implementation of this proposed rule. This means we assume there will be costs related to training in the first year of analysis. The Coast Guard requests comment on the ability of affected owners and operators to develop and provide relevant cybersecurity training within the first year of implementation.

Based on information from the Jones Walker "Ports and Terminals Cybersecurity Survey," (see footnote 69), about 25 percent of facilities are currently conducting cybersecurity training on an annual basis.[78] Therefore, we estimate the number of facility and OCS facility owners and operators needing to implement training to be about 1,281 (1,708 owners and operators × 0.75).

Based on information from CISA's SMEs, we assume that the CySO at a facility or OCS facility would spend 2 hours per year to develop, update, and provide cybersecurity training. SMEs at CISA also estimate that it would take 1 hour per facility employee to complete the training annually, based on existing industry-leading cyber awareness training programs. This proposed rule would also require part-time employees and contractors to complete the training. However, the Coast Guard has data only on the

[78] See footnote 69 and page 48 of the survey in the docket.

number of full-time employees at facilities and OCS facilities, so we use this estimate with the acknowledgement that costs may be higher for facilities than we estimate in this analysis if we take other employees into account, such as part-time employees and contractors. As before, we use the estimate of the average number of employees at facilities and OCS facilities, or 74.

To obtain the unloaded mean hourly wage rate of employees at facilities and OCS facilities, we use BLS's Quarterly Census of Employment and Wages (QCEW) data. We also use the North American Industry Classification System (NAICS) code for "Port and Harbor Operations," which is 488310, to obtain the representative hourly wage for employees at facilities and OCS facilities. The BLS reports the weekly wage to be $1,653.[79] Dividing this value by the standard number of hours in a work week, or 40, we obtain the unloaded hourly wage rate of approximately $41.33. We once again apply a load factor of 1.46 to this wage to obtain a loaded mean hourly wage rate for facility employees of approximately $60.34 (($1,653 ÷ 40 hours) × 1.46)).

We estimate the undiscounted initial-year and annual cost for facility and OCS facility owners and operators to train employees on aspects of cybersecurity to be approximately $5,935,437, rounded [1,281 facility owners and operators × ((74 employees at each facility company × $60.34 × 1 hour) + (1 CySO developing training × $84.14 × 2 hours))].

We estimate the discounted cost for facility and OCS facility owners and operators to complete annual training to be approximately $41,688,025 over a 10-year

[79] Readers can access this webpage at www.bls.gov/cew/. In the menu at the top of the page, readers should use the dropdown menu under "QCEW Data," and select "Databases." Doing this will bring the reader to https://www.bls.gov/cew/data.htm. On this page, select the multi-screen tool (https://data.bls.gov/cgi-bin/dsrv?en). On screen 1, select "488310 NAICS 488310 Port and harbor operations." On screen 2, select "US000 U.S. TOTAL." Select "5 Private," "4 Average Weekly Wage," and "0 All establishment sizes" on screens 3, 4, and 5, respectively. Screen 6 shows the relevant Series ID (ENUUS000405488310). Select "Retrieve Data." Please consider that 2022 data from QCEW are preliminary and may change from the estimate in the text. For the purposes of this analysis, we used Q1 2022 QCEW data. Accessed on July 13, 2023.

period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $5,935,437, using a 7-percent discount rate. See table 18.

Table 18: Estimated Training Costs of the Proposed Rule for Facility and OCS Facility Owners and Operators (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Total Cost	7%	3%
1	$5,935,437	$5,547,137	$5,762,560
2	$5,935,437	$5,184,241	$5,594,719
3	$5,935,437	$4,845,085	$5,431,766
4	$5,935,437	$4,528,116	$5,273,559
5	$5,935,437	$4,231,885	$5,119,960
6	$5,935,437	$3,955,032	$4,970,835
7	$5,935,437	$3,696,292	$4,826,053
8	$5,935,437	$3,454,478	$4,685,489
9	$5,935,437	$3,228,484	$4,549,018
10	$5,935,437	$3,017,275	$4,416,523
Total	$59,354,370	**$41,688,025**	**$50,630,482**
Annualized		**$5,935,437**	**$5,935,437**

Note: Totals may not sum due to independent rounding.

Employees on board U.S.-flagged vessels would also be required to complete annual cybersecurity training. The hour estimates for the CySO to develop cybersecurity training and employees to complete the training are the same as for facility estimates, 2 hours and 1 hour, respectively. The training costs for U.S.-flagged vessels are based upon the number of employees for each vessel type, similar to the cost analysis for account security measures. We chose several representative labor categories of vessel employees based on the manning requirements listed in the certificates of inspection for each vessel. From the BLS OEWS program, we use the labor categories, "Captains, Mates, and Pilots of Water Vessels," with an occupational code of 53-5021, "Sailors and Marine Oilers," with an occupational code of 53-5011, and "Ship Engineers," with an occupational code of 53-5031.[80] The unloaded mean hourly wage rates from May 2022 for these occupations are $50.09, $25.65, and $48.55, respectively. We also use an

[80] See https://www.bls.gov/oes/2022/may/oes_nat.htm#00-0000 for 2022 wage rates associated with the listed occupations. Accessed September 9, 2023.

assortment of labor categories to estimate a mean hourly wage for the industrial personnel identified in the certificate of inspection for MODUs in the affected population. According to SMEs with CG-CVC, industrial personnel aboard MODUs generally include a mixture of hotel and steward staff; laborers and riggers; specialized technicians; and mechanics, electricians, and electronic technicians for maintenance. For these groups, we find a combined unloaded weighted mean hourly wage of $25.16. For each vessel type, we weight the representative wages based on the average occupational ratios across vessels in the population. See Appendix A: Wages Across Vessel Types, for more details on how the industrial personnel and weighted mean hourly wages for each vessel type were calculated.[81] We apply the same load factor we used previously in this analysis, 1.46, to these wage rates, to obtain the loaded mean hourly wage rates shown in table 19. [82]

Table 19: Estimated Weighted Mean Hourly Wage Rates for Employees Aboard U.S.-flagged Vessels[83]

Vessel Type	Loaded Weighted Mean Hourly Wage
MODU	$39.60
Subchapter I Vessels	$46.36
OSVs	$54.92
Subchapter H Passenger Vessels	$41.85
Subchapter K Passenger Vessels	$45.52
Subchapter M Towing Vessels	$51.28
Subchapter D and Combination Subchapters O&D Tank Vessels	$55.94
Subchapters K and T International Passenger Vessels	$44.59

[81] It should be noted that the wage calculations in Appendix A: Wages Across Vessel Types are conducted with occupational ratios based on employee counts without the 1.33 shoreside employee modifier applied. Applying this multiplier evenly across all the employee counts would not have an impact on the occupational ratios, and thus would not impact our estimated weighted mean hourly wages. Because we do not have a good grasp on what occupations the shoreside employees would have, we simply apply the weighted mean hourly wages to all employees in the give population of vessels.
[82] See footnote 71.
[83] See Appendix A: Wages Across Vessel Types for more information on how these wages rates were calculated.

We estimate the undiscounted initial-year and annual cost of cybersecurity training for vessel employees to be approximately $6,166,909 (number of vessels for each affected vessel category × number of employees for each vessel type × representative mean hourly wage for vessel type × 1 hours for training). For example, using OSVs, there are about 426 OSVs, with 16 employees for each OSV. Therefore, we estimate the annual training cost for OSVs to be about $374,335 (426 OSVs × 16 employees × $54.92 × 1 hour), rounded. We perform this calculation for all for the affected vessel types in this proposed rule and add it to the estimated costs for training development. We estimate the undiscounted annual cost to develop cybersecurity training to be approximately $269,585 (1,602 vessel companies × 1 CySO per vessel company × $84.14 × 2 hours to develop training)]. This means the total undiscounted annual training cost for the affected population of U.S.-flagged vessels is $6,436,494 ($6.166,909 employee training costs + $269,585 training development costs). Table 20 displays the total employee training costs for each vessel type impacted by the proposed training requirement.

Table 20. Estimated Training Costs of the Proposed Rule for U.S.-Flagged Vessels by Type (2022 Dollars)

Vessel Type	Number of Vessels	Number of Employees (Includes Shoreside)	Trainee Wage	Total
MODU	1	372	$39.60	$14,731
Subchapter I Vessels	574	82	$46.36	$2,182,072
OSVs	426	16	$54.92	$374,335
Subchapter H Passenger Vessels	34	85	$41.85	$120,947
Subchapter K Passenger Vessels	379	35	$45.52	$603,823
Subchapter M Towing Vessels	3921	13	$51.28	$2,613,895
Subchapter D and Combination Subchapters O&D Tank Vessels	88	40	$55.94	$196,909
Subchapters K and T International Passenger Vessels	50	27	$44.59	$60,197

Total				**$6,166,909**

Note: Totals may not sum due to independent rounding.

We estimate the discounted cost for employees aboard U.S.-flagged vessels to complete annual cybersecurity training to be approximately $45,207,239 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $6,436,494, using a 7-percent discount rate. See table 21.

Table 21: Estimated Training Costs of the Proposed Rule for U.S.-Flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Total Cost	7%	3%
1	$6,436,494	$6,015,415	$6,249,023
2	$6,436,494	$5,621,883	$6,067,013
3	$6,436,494	$5,254,096	$5,890,304
4	$6,436,494	$4,910,370	$5,718,742
5	$6,436,494	$4,589,131	$5,552,176
6	$6,436,494	$4,288,908	$5,390,462
7	$6,436,494	$4,008,325	$5,233,459
8	$6,436,494	$3,746,098	$5,081,028
9	$6,436,494	$3,501,026	$4,933,037
10	$6,436,494	$3,271,987	$4,789,356
Total	$64,364,940	**$45,207,239**	**$54,904,600**
Annualized		**$6,436,494**	**$6,436,494**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of cybersecurity training for facilities and vessels to be approximately $86,895,266 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $12,371,931, using a 7-percent discount rate. See table 22.

Table 22: Summary of Training Costs of the Proposed Rule for U.S.-Flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facilities and OCS Facilities	U.S.-Flagged Vessels	Total Cost	7%	3%
1	$5,935,437	$6,436,494	$12,371,931	$11,562,552	$12,011,583
2	$5,935,437	$6,436,494	$12,371,931	$10,806,124	$11,661,732
3	$5,935,437	$6,436,494	$12,371,931	$10,099,181	$11,322,069
4	$5,935,437	$6,436,494	$12,371,931	$9,438,487	$10,992,300
5	$5,935,437	$6,436,494	$12,371,931	$8,821,016	$10,672,136
6	$5,935,437	$6,436,494	$12,371,931	$8,243,940	$10,361,297

7	$5,935,437	$6,436,494	$12,371,931	$7,704,617	$10,059,512
8	$5,935,437	$6,436,494	$12,371,931	$7,200,576	$9,766,517
9	$5,935,437	$6,436,494	$12,371,931	$6,729,511	$9,482,055
10	$5,935,437	$6,436,494	$12,371,931	$6,289,262	$9,205,879
Total	**$59,354,370**	**$64,364,940**	**$123,719,310**	**$86,895,266**	**$105,535,080**
Annualized				**$12,371,931**	**$12,371,931**

Note: Totals may not sum due to independent rounding.

Penetration Testing

The third proposed provision under cybersecurity measures that would impose costs on industry is penetration testing, in proposed § 101.650(e)(2). The CySO for each U.S.-flagged vessel, facility, and OCS facility would ensure that a penetration test is completed in conjunction with renewing the FSP, VSP, or OCS FSP. We assume facility and vessel owners and operators in the affected population would pay a third party to conduct a penetration test to maintain safety and security within the IT and OT systems for all KEVs. The cost for penetration testing is a function of the number of vessel and facility owners and operators, because networks are typically managed at a corporate level. At the conclusion of the test, the CySO would also need to document all identified vulnerabilities in the FSA, OCS FSP, or VSA—a cost that is included in our analysis of annual Cybersecurity Plan maintenance. Further, it is expected that the CySO would also work to correct or mitigate the identified vulnerabilities. However, the methods employed and time taken to correct or mitigate these vulnerabilities represent a source of uncertainty in our analysis, and we are unable to estimate the associated costs.

Based on the Jones Walker survey (see footnote number 69), 68 percent of facilities and OCS facilities are currently conducting penetration testing. Using 1,708 affected facility owners and operators, the number of facility and OCS facility owners and operators needing to conduct penetration testing is about 547 (1,708 × 0.32). Using cost estimates for penetration testing from NMSAC members who have experience conducting and contracting with facilities and OCS facilities to conduct penetration tests, we estimate it would cost each facility owner or operator $5,000 for the initial penetration

test and an additional $50 for each employee's Internet Protocol (IP) address,[84] to capture the additional costs of network complexity. The number of employees for each facility is 74. Facility and OCS facility owners and operators would incur penetration testing costs in conjunction with submitting and renewing the Cybersecurity Plan, or every 5 years. This means penetration testing costs would be incurred in the second and seventh year of analysis. We estimate the undiscounted second- and seventh-year costs to facilities and OCS facilities for penetration testing to be about $4,758,900 [(547 facility owners and operators × $5,000) + (74 employees × 547 facility owners and operators × $50)]. We estimate the discounted cost for owners and operators of facilities and OCS facilities to conduct penetration testing to be about $7,120,212 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be about $979,477 using a 7-percent discount rate. See table 23.

Table 23: Estimated Penetration Testing Costs of the Proposed Rule for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Facilities	Number of Employees per Facility	Cost of Penetration Test	Cost per IP Address	Total Cost	7%	3%
1	0	0	$0	$0	$0	$0	$0
2	547	74	$5,000	$50	$4,758,900	$4,156,608	$4,485,720
3	0	0	$0	$0	$0	$0	$0
4	0	0	$0	$0	$0	$0	$0
5	0	0	$0	$0	$0	$0	$0
6	0	0	$0	$0	$0	$0	$0
7	547	74	$5,000	$50	$4,758,900	$2,963,604	$3,869,421
8	0	0	$0	$0	$0	$0	$0
9	0	0	$0	$0	$0	$0	$0
10	0	0	$0	$0	$0	$0	$0
Total					**$9,517,800**	**$7,120,212**	**$8,355,141**
Annualized						**$1,013,758**	**$979,477**

Note: Totals may not sum due to independent rounding.

[84] An IP address is a unique numerical identifier for each device or network that connects to the internet. Because we do not have data on the number of devices each organization uses, we use the number of employees as a proxy because each employee could have a device using the organizational network.

Owners and operators of U.S.-flagged vessels would also need to conduct penetration testing, similar to facilities. We do not include barges or barge-specific owners and operators, given the unmanned nature of barges and their relatively limited onboard IT and OT systems. All estimates for vessel penetration testing are the same as for facilities and OCS facilities. We estimate the undiscounted second- and seventh-year costs for owners and operators of vessels to conduct penetration testing to be approximately $14,322,700 [(1,602 vessel owners and operators × $5,000) + (number of vessels for each vessel type × number of employees for each vessel type × $50)]. See table 24 for a calculation of the costs per IP address for the various vessel populations, which can be added to the costs per owner or operator costs, or $8,010,000 (1,602 owners and operators × $5,000) in years 2 and 7.

Table 24: Estimated Penetration Testing Costs of the Proposed Rule for U.S.-Flagged Vessels by Vessel Type (2022 Dollars, Undiscounted)

Vessel Type	Number of Vessels	Number of Employees per Vessel	Cost per IP Address	Total for Population
MODU	1	372	$50	$18,600
Subchapter I Vessels	574	82	$50	$2,353,400
OSVs	426	16	$50	$340,800
Subchapter H Passenger Vessels	34	85	$50	$144,500
Subchapter K Passenger Vessels	379	35	$50	$663,250
Subchapter M Towing Vessels	3921	13	$50	$2,548,650
Subchapter D and Combination Subchapters O&D Tank Vessels	88	40	$50	$176,000
Subchapters K and T International Passenger Vessels	50	27	$50	$67,500
Total				**$6,312,700**

Note: Totals may not sum due to independent rounding.

We estimate the discounted cost for owners and operators of vessels to conduct penetration testing to be approximately $21,429,459 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $3,051,073 using a 7-percent discount rate. See table 25.

Table 25: Estimated Penetration Testing Costs of the Proposed Rule for Population of U.S.-Flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Total Cost	7%	3%
1	$0	$0	$0
2	$14,322,700	$12,510,001	$13,500,518
3	$0	$0	$0
4	$0	$0	$0
5	$0	$0	$0
6	$0	$0	$0
7	$14,322,700	$8,919,458	$11,645,666
8	$0	$0	$0
9	$0	$0	$0
10	$0	$0	$0
Total	**$28,645,400**	**$21,429,459**	**$25,146,184**
Annualized		**$3,051,073**	**$2,947,900**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost to conduct penetration testing for owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to be approximately $28,549,669 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $4,064,831 using a 7-percent discount rate. See table 26.

Table 26: Estimated Penetration Testing Costs of the Proposed Rule for Facilities, OCS Facilities, and U.S.-Flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facilities and OCS Facilities Cost	U.S.-Flagged Vessel Cost	Total Cost	7 Percent	3 Percent
1	$0	$0	$0	$0	$0
2	$4,758,900	$14,322,700	$19,081,600	$16,666,608	$17,986,238
3	$0	$0	$0	$0	$0
4	$0	$0	$0	$0	$0
5	$0	$0	$0	$0	$0
6	$0	$0	$0	$0	$0
7	$4,758,900	$14,322,700	$19,081,600	$11,883,061	$15,515,087
8	$0	$0	$0	$0	$0
9	$0	$0	$0	$0	$0
10	$0	$0	$0	$0	$0
Total	**$9,517,800**	**$28,645,400**	**$38,163,200**	**$28,549,669**	**$33,501,325**
Annualized				**$4,064,831**	**$3,927,377**

Note: Totals may not sum due to independent rounding.

Resilience

The fourth cost provision under cybersecurity measures would be resilience, in proposed § 101.650(g). Each CySO for a facility, OSC facility, and U.S.-flagged vessel would be required to report any cyber incident to the NRC, develop a Cyber Incident Response Plan, validate the effectiveness of Cybersecurity Plans through annual tabletop exercises or periodic reviews of incident response cases, and perform backups of critical IT and OT systems. Of these proposed requirements, the costs associated development of a Cyber Incident Response Plan are already captured in the overall costs to develop the Cybersecurity Plan, and any subsequent annual maintenance for the Cyber Incident Response Plan would be captured in the costs for annual maintenance of the Cybersecurity Plan. In addition, costs associated with validating and conducting exercise of Cybersecurity Plans through annual tabletop exercises or periodic reviews of incident response cases is already captured in the costs estimated for drills and exercises in proposed § 101.635.

To estimate the costs associated with cyber incident reporting, the Coast Guard uses historical cyber incident reporting data from the NRC. From 2018 to 2022, the NRC fielded and processed an average of 18 cyber incident reports from facilities and OCS facilities, and an average of 2 cyber incident reports from U.S.-flagged vessels, for a total of 20 cyber incident reports per year. While we anticipate that this number could increase or decrease following the publication of a rule focused on cybersecurity standards and procedures, we use the historical averages to estimate costs for the affected population.[85] Due to the uncertainty surrounding how these regulatory changes may

[85] The Coast Guard believes that cyber incident reports could increase following publication of this NPRM due to greater enforcement of reporting procedures and greater awareness surrounding the need to report. However, the Coast Guard acknowledges that cyber incident reports could also decrease because greater prevention measures would be implemented because of this proposed rule. As a result, we use historical cyber incident reporting data to analyze costs moving forward.

impact the number of incident reports made in the future, the Coast Guard requests comment on the expected number of incident reports submitted each year.

For both the population of facilities and OCS facilities and the population of U.S.-flagged vessels, we assume that it will take 8.5 minutes (0.15 hours) of a CySO's time to report a cyber incident to the NRC. We base this estimated hour burden on the time to report suspicious maritime activity to the NRC in currently approved OMB ICR, Control Number 1625-0096 titled "Report of Oil or Hazardous Substance Discharge and Report of Suspicious Maritime Activity." For the population of facilities and OCS facilities, we estimate annual undiscounted costs of $227 (18 cyber incident reports × 0.15 hours to report × $84.14 CySO wage). We estimate the discounted cost for owners and operators of facilities and OCS facilities to report cyber incidents to be about $1,592 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be about $227 using a 7-percent discount rate. See table 27.

Table 27: Estimated Cyber Incident Reporting Costs of the Proposed Rule for the Population of Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Incident Reports Per Year	CySO Wage	Hours to Report Incident	Total Cost	7%	3%
1	18	$84.14	0.15	$227	$212	$220
2	18	$84.14	0.15	$227	$198	$214
3	18	$84.14	0.15	$227	$185	$208
4	18	$84.14	0.15	$227	$173	$202
5	18	$84.14	0.15	$227	$162	$196
6	18	$84.14	0.15	$227	$151	$190
7	18	$84.14	0.15	$227	$141	$185
8	18	$84.14	0.15	$227	$132	$179
9	18	$84.14	0.15	$227	$123	$174
10	18	$84.14	0.15	$227	$115	$169
Total				**$2,270**	**$1,592**	**$1,937**
Annualized				**$227**	**$227**	**$227**

Note: Totals may not sum due to independent rounding.

For the population of U.S.-flagged vessels, we estimate annual undiscounted costs of $25 (2 cyber incident reports × 0.15 hours to report × $84.14 CySO wage). We

estimate the discounted cost for owners and operators of facilities and OCS facilities to report cyber incidents to be about $250 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be about $25 using a 7-percent discount rate. See table 28.

Table 28: Estimated Cyber Incident Reporting Costs of the Proposed Rule for the Population of U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Incident Reports Per Year	CySO Wage	Hours to Report Incident	Total Cost	7%	3%
1	2	$84.14	0.15	$25	$23	$24
2	2	$84.14	0.15	$25	$22	$24
3	2	$84.14	0.15	$25	$20	$23
4	2	$84.14	0.15	$25	$19	$22
5	2	$84.14	0.15	$25	$18	$22
6	2	$84.14	0.15	$25	$17	$21
7	2	$84.14	0.15	$25	$16	$20
8	2	$84.14	0.15	$25	$15	$20
9	2	$84.14	0.15	$25	$14	$19
10	2	$84.14	0.15	$25	$13	$19
Total				**$250**	**$177**	**$214**
Annualized				**$25**	**$25**	**$25**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost for owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to be approximately $1,771 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $252 using a 7-percent discount rate. See table 29.

Table 29: Estimated Cyber Incident Reporting Costs of the Proposed Rule for the Population of Facilities, OCS Facilities, and U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facilities	Vessels	Total Cost	7%	3%
1	$227	$25	$252	$236	$245
2	$227	$25	$252	$220	$238
3	$227	$25	$252	$206	$231
4	$227	$25	$252	$192	$224
5	$227	$25	$252	$180	$217
6	$227	$25	$252	$168	$211
7	$227	$25	$252	$157	$205
8	$227	$25	$252	$147	$199

9	$227	$25	$252	$137	$193
10	$227	$25	$252	$128	$188
Total			**$2,520**	**$1,771**	**$2,151**
Annualized				**$252**	**$252**

Note: Totals may not sum due to independent rounding.

The Coast Guard does not have data on the IT resources that owners and operators would need to back up data, either internally or externally. Coast Guard SMEs indicate that most of the affected population is likely already performing data backups. The time burden of backing up data is minimal because they can occur in the background through automated processes, making any new costs a function of data storage space. The external storage of data would require cloud storage (storage on an external server), and the cost would be dependent upon the capacity needed; for example, 1 terabyte or 100 terabytes of space. These costs would likely be incurred on a monthly basis, although we do not know how much additional data space a given owner or operator would need, if any. Coast Guard SMEs with CG-CYBER indicate that the current market prices for cloud storage subscriptions range from $21 to $41 per month for 1 terabyte of data, $54 to $320 per month for 10 terabytes, and up to $402 to $3200 per month for 100 terabytes of data. There may also be costs associated with the encryption of data that we are not able to estimate in this analysis. The Coast Guard requests public comment on the costs associated with data backup storage and protection.

Routine System Maintenance for Risk Management

The final cost provision under cybersecurity measures would be routine system maintenance for risk management, in proposed § 101.650(e)(3)(i) through (vi). This proposed rule would require the CySO of a U.S.-flagged vessel, facility, or OCS facility to ensure patching (software updates) or implementing controls for all KEVs in critical IT and OT systems in paragraph (e)(3)(i), maintain a method to receive or act on publicly submitted vulnerabilities in paragraph (e)(3)(ii), maintain a method to share threat and vulnerability information with external stakeholders in paragraph (e)(3)(iii), ensure there

are no exploitable channels exposed to internet accessible systems in paragraph (e)(3)(iv), ensure that no OT is connected to the publicly accessible internet unless explicitly required for operation in paragraph (e)(3)(v), and conduct vulnerability scans according to the Cybersecurity Plan in paragraph (e)(3)(vi).

Based on information from CGCYBER and NMSAC, we estimate costs for only the vulnerability scans in this analysis, because it is expected that CySOs will incorporate many of these provisions into the initial development and annual maintenance of the Cybersecurity Plan. Provisions that require setting up routine patching, developing methods for communicating vulnerabilities, and ensuring limited network connectivity of OT and other exploitable systems are expected to be less time-intensive efforts that will be completed following an initial Cybersecurity Assessment and documented in the Cybersecurity Plan. As a result, we include those costs in that portion of the analysis. However, if an OT system does need to be taken offline or segmented from other IT systems, the Coast Guard does not have information on how long or intensive that process would be because of the great degree of variability in OT systems within the affected population.

We discuss network segmentation and uncertainty more in later sections in this NPRM. We request public comment on the expected costs of network segmentation, particularly from those in the affected population who have completed these processes in the past.

Based on information from CGCYBER, the cost to acquire third-party software capable of vulnerability scans would be approximately $3,390 annually (which includes the software subscription cost) for each U.S.-flagged vessel, facility, and OCS facility. We base our analysis on the cost of a prevalent vulnerability scanner or virus software for business. Vulnerability scans can occur in the background while systems are operational and represent a less intensive method of monitoring IT and OT systems for

vulnerabilities, which complements more intensive penetration tests that would be required every 5 years. For this reason, we do not estimate an hour burden in addition to the annual subscription cost of securing vulnerability scanning software. We estimate the undiscounted annual cost for facility owners and operators to subscribe to and use vulnerability scanning software to be approximately $5,790,120 (1,708 facility owners and operators × $3,390). We estimate the undiscounted annual cost for vessel owners and operators to subscribe to and use vulnerability scanning software to be approximately $5,430,780 (1,602 vessel owners and operators × $3,390). Combined, we estimate the total discounted cost for owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to use vulnerability scanning software to be approximately $78,810,907 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $11,220,900, using a 7-percent discount rate. See table 30.

Table 30: Estimated Vulnerability Scanning Software Costs of the Proposed Rule for Facilities, OCS Facilities, and U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facility and OCS Facility Costs	U.S.-flagged Vessel Costs	Total Cost	7%	3%
1	$5,790,120	$5,430,780	$11,220,900	$10,486,822	$10,894,078
2	$5,790,120	$5,430,780	$11,220,900	$9,800,769	$10,576,774
3	$5,790,120	$5,430,780	$11,220,900	$9,159,597	$10,268,713
4	$5,790,120	$5,430,780	$11,220,900	$8,560,371	$9,969,624
5	$5,790,120	$5,430,780	$11,220,900	$8,000,347	$9,679,247
6	$5,790,120	$5,430,780	$11,220,900	$7,476,959	$9,397,327
7	$5,790,120	$5,430,780	$11,220,900	$6,987,813	$9,123,619
8	$5,790,120	$5,430,780	$11,220,900	$6,530,666	$8,857,882
9	$5,790,120	$5,430,780	$11,220,900	$6,103,426	$8,599,886
10	$5,790,120	$5,430,780	$11,220,900	$5,704,137	$8,349,403
Total			$112,209,000	**$78,810,907**	**$95,716,553**
Annualized			$11,220,900	**$11,220,900**	**$11,220,900**

Note: Totals may not sum due to independent rounding.

Total Costs of the Proposed Rule to Industry

We estimate the total discounted cost of this proposed rule to the affected population of facilities and OCS facilities to be approximately $221,437,074 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $31,527,658, using a 7-percent discount rate. See table 31.

Table 31: Summary of Total Discounted Costs of the Proposed Rule for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Cybersecurity Plan Costs	Drills and Exercises Costs	Account Security and Multifactor Authentication Costs	Training Costs	Penetration Testing Costs	Vulnerability Management Costs	Cyber Incident Reporting Costs	Total Costs	7%	3%
1	$14,350,077	$1,437,111	$5,956,801	$5,935,437	$0	$5,790,120	$227	$33,469,773	$31,280,162	$32,494,925
2	$15,784,664	$1,437,111	$3,346,801	$5,935,437	$4,758,900	$5,790,120	$227	$37,053,260	$32,363,752	$34,926,251
3	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$25,190,767	$28,241,064
4	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$23,542,773	$27,418,509
5	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$22,002,592	$26,619,911
6	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$20,563,170	$25,844,574
7	$4,520,211	$1,437,111	$3,346,801	$5,935,437	$4,758,900	$5,790,120	$227	$25,788,807	$16,059,973	$20,968,660
8	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$17,960,669	$24,360,990
9	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$16,785,672	$23,651,446
10	$14,350,077	$1,437,111	$3,346,801	$5,935,437	$0	$5,790,120	$227	$30,859,773	$15,687,544	$22,962,569
Total	**$135,105,491**	**$14,371,110**	**$36,078,010**	**$59,354,370**	**$9,517,800**	**$57,901,200**	**$2,270**	**$312,330,251**	**$221,437,074**	**$267,488,899**
Annualized								**$31,233,025**	**$31,527,658**	**$31,357,859**
Percent of Total	43.26%	4.60%	11.55%	19.00%	3.05%	18.54%	0.00%	100.00%	-	-

Note: Totals may not sum due to independent rounding

As seen in table 31, the primary cost drivers for the population of facilities and OCS facilities are Cybersecurity Plan-related costs (development, resubmission, maintenance, and audits) at 43.26 percent of the total costs to industry. Cybersecurity training and vulnerability management costs come in second and third at 19 percent and 18.54 percent of the total costs, respectively. We believe some of this is due to the analysis of Cybersecurity Plan costs and vulnerability management costs, which assumes no baseline activity within the affected population because of a lack of information. Costs that appear as a higher percentage of the total costs in the population of U.S.-flagged vessels (account security and multifactor authentication, for example) have been adjusted based on current baseline activity within the population of facilities based on survey results, and thus, appear as smaller impacts to the population in general.

We estimate the total discounted cost of this proposed rule to the affected population of U.S.-flagged vessels to be approximately $313,656,415 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $44,657,617, using a 7-percent discount rate. See table 32.

Table 32: Summary of Total Costs of the Proposed Rule for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7-percent Discount Rate)

Year	Cybersecurity Plan Costs	Drills and Exercises Costs	Account Security and Multifactor Authentication Costs	Training Costs	Penetration Testing Costs	Vulnerability Management Costs	Cyber Incident Reporting Costs	Total Costs	7 Percent	3 Percent
1	$5,973,940	$1,493,485	$34,278,339	$6,436,494	$0	$5,430,780	$25	$53,613,063	$50,105,666	$52,051,517
2	$6,573,017	$1,493,485	$19,860,339	$6,436,494	$14,322,700	$5,430,780	$25	$54,116,840	$47,267,744	$51,010,312
3	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$32,970,150	$36,962,435
4	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$30,813,224	$35,885,859
5	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$28,797,406	$34,840,640
6	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$26,913,463	$33,825,864
7	$1,882,044	$1,493,485	$19,860,339	$6,436,494	$14,322,700	$5,430,780	$25	$49,425,867	$30,779,946	$40,187,753
8	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$23,507,261	$31,884,121
9	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$21,969,403	$30,955,458
10	$7,168,728	$1,493,485	$19,860,339	$6,436,494	$0	$5,430,780	$25	$40,389,851	$20,532,152	$30,053,842
Total	**$64,610,097**	**$14,934,850**	**$213,021,390**	**$64,364,940**	**$28,645,400**	**$54,307,800**	**$250**	**$439,884,727**	**$313,656,415**	**$377,657,801**
Annualized								**$43,988,473**	**$44,657,617**	**$44,273,015**
Percent of Total	14.69%	3.40%	48.43%	14.63%	6.51%	12.35%	0.00%	100.00%	-	-

Note: Totals may not sum due to independent rounding.

As in table 32, the primary cost drivers for the population of U.S.-flagged vessels are costs related to account security and multifactor authentication at 48.43 percent of the total costs to industry. Costs related to the Cybersecurity Plan and cybersecurity training come in second and third at 14.69 percent and 14.63 percent of the total costs, respectively. We estimate that account security and multifactor authentication costs represent such a high portion of the overall costs related to cybersecurity because the Coast Guard was unable to estimate current baseline activity for these provisions and used conservative (upper-bound) estimates related to the costs of implementing and managing multifactor authentication. As a result, the Coast Guard requests public comment on who in the affected population of U.S.-flagged vessels has already implemented multifactor authentication and what the associated costs were.

We estimate the total discounted cost of this proposed rule to industry to be approximately $535,093,488 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $76,185,275, using a 7-percent discount rate. See table 33.

Table 33: Summary of Total Costs of the Proposed Rule to Industry (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rate)

Year	Cybersecurity Plan Costs	Drills and Exercises Costs	Account Security and Multifactor Authentication Costs	Training Costs	Penetration Testing Costs	Vulnerability Management Costs	Cyber Incident Reporting Costs	Total Costs	7 Percent	3 Percent
1	$20,324,017	$2,930,596	$40,235,140	$12,371,931	$0	$11,220,900	$252	$87,082,836	$81,385,828	$84,546,443
2	$22,357,681	$2,930,596	$23,207,140	$12,371,931	$19,081,600	$11,220,900	$252	$91,170,100	$79,631,496	$85,936,563
3	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$58,160,917	$65,203,499
4	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$54,355,997	$63,304,368
5	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$50,799,997	$61,460,552
6	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$47,476,633	$59,670,438
7	$6,402,255	$2,930,596	$23,207,140	$12,371,931	$19,081,600	$11,220,900	$252	$75,214,674	$46,839,919	$61,156,413
8	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$41,467,930	$56,245,111
9	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$38,755,075	$54,606,904
10	$21,518,805	$2,930,596	$23,207,140	$12,371,931	$0	$11,220,900	$252	$71,249,624	$36,219,696	$53,016,412
Total								**$752,214,978**	**$535,093,488**	**$645,146,703**
Annualized								**$75,221,498**	**$76,185,275**	**$75,630,875**
Percent of Total	26.55%	3.90%	33.12%	16.45%	5.07%	14.92%	0.00%	100.00%	-	-

Note: Totals may not sum due to independent rounding.

Total Costs of the Proposed Rule per Affected Owner or Operator

We estimate the average annual cost per owner or operator of a facility or OCS facility to be approximately $27,589, under the assumption that an owner or operator would need to implement each of the provisions required by this proposed rule. Each additional facility owned or operated would increase the estimated annual costs by an average of $4,396 per facility, since each facility or OCS facility will require an individual Cybersecurity Plan. Year 2 of the analysis period represents the year with the highest costs incurred per owner, with estimated costs of $37,667 for an owner or operator with one facility or OCS facility. See table 34 for a breakdown of the costs per entity for an owner or operator owning one facility or OCS facility.

Table 34: Summary of Total Costs of the Proposed Rule per Owner or Operator of a Facility or OCS Facility (2022 Dollars, 10-year Undiscounted Costs)[86]

Year	Facility Count	Cybersecurity Plan	Drills and Exercises	Account Security Measures	Multifactor Authentication	Cybersecurity Training	Penetration Testing	Vulnerability Management	Cyber Incident Reporting	Total
1	1	$4,207	$841	$576	$20,100	$4,633	$0	$3,390	$13	$33,760
2	1	$8,414	$841	$576	$11,100	$4,633	$8,700	$3,390	$13	$37,667
3	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
4	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
5	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
6	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
7	1	$1,893	$841	$576	$11,100	$4,633	$8,700	$3,390	$13	$31,146
8	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
9	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
10	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
Total										**$275,893**
Average										**$27,589**

Note: Totals may not sum due to independent rounding.

[86] The cost totals in table 34 represent cost estimates for owners and operators of 1 facility or OCS facility under the assumption that they will need to implement all cost-creating provisions of the proposed rule. Therefore, when multiplied over the full number of affected entities, the calculated totals will exceed those estimated for the population of facilities and OCS facilities elsewhere in the analysis. In addition, the cost estimates for items related to the Cybersecurity Plan are dependent upon the number of facilities owned and must be multiplied accordingly by the number of facilities owned. This is discussed in further detail later in the analysis of costs per owner or operator.

To estimate the cost for an owner or operator of a facility or OCS facility to develop, resubmit, conduct annual maintenance, and audit the Cybersecurity Plan, we use estimates provided earlier in the analysis. The hour-burden estimates are 100 hours for developing the Cybersecurity Plan (average hour burden), 10 hours for annual maintenance of the Cybersecurity Plan (which would include amendments), 15 hours to renew Cybersecurity Plans every 5 years, and 40 hours to conduct annual audits of Cybersecurity Plans.

Based on estimates from Coast Guard FSP and OCS FSP reviewers at local inspections offices, approximately 10 percent of Cybersecurity Plans would need to be resubmitted in the second year due to revisions that would be needed to the Plans, which is consistent with the current resubmission rate for FSPs and OCS FSPs. For renewals of Plans after 5 years (occurring in the seventh year of the analysis period), Plans would need to be further revised and resubmitted in approximately 10 percent of cases as well. However, in this portion of the analysis, we estimate costs as though the owner or operator will need to revise and resubmit their Plans in all cases, resulting in an upper-bound (high) estimate of per-entity costs. We estimate the time for revision and resubmission to be about half the time to develop the Plan itself, or 50 hours in the second year of submission, and 7.5 hours after 5 years (in the seventh year of the analysis period). Because we include the annual Cybersecurity Assessment in costs to develop Plans, and we do not assume that owners and operators will wait until the second year of analysis to begin developing the Cybersecurity Plan or implementing relevant cybersecurity measures, we divide the estimated 100 hours to develop Plans equally across the first and second years of analysis.

Using the CySO loaded hourly CySO wage of $84.14, we estimate the Cybersecurity Plan-related costs by adding the total number of hours to develop, resubmit, maintain, and audit each year and multiplying by the CySO wage. For

example, we estimate owners would incur $8,414 in costs in year 2 of the analysis period [1 facility × $84.14 CySO wage × (50 hours to develop the Plan + 50 hours to revise and resubmit the Plan) = $8,414]. Table 35 displays the per-entity cost estimates for an owner or operator of 1 facility or OCS facility over a 10-year period of analysis. For an owner or operator of multiple facilities or OCS facilities, we estimate the total costs by multiplying the total costs in table 35 by the number of owned facilities.

Table 35: Cybersecurity Plan-Related Costs per Owner or Operator of a Facility or OCS Facility (2022 Dollars, 10-year Undiscounted Costs)

Year	Facility Count	CySO Wage	Hours to Develop Plan	Hours to Resubmit Plan	Annual Maintenance Hours	Audit Hours	Total
1	1	$84.14	50	0	0	0	$4,207
2	1	$84.14	50	50	0	0	$8,414
3	1	$84.14	0	0	10	40	$4,207
4	1	$84.14	0	0	10	40	$4,207
5	1	$84.14	0	0	10	40	$4,207
6	1	$84.14	0	0	10	40	$4,207
7	1	$84.14	15	7.5	0	0	$1,893
8	1	$84.14	0	0	10	40	$4,207
9	1	$84.14	0	0	10	40	$4,207
10	1	$84.14	0	0	10	40	$4,207
Total							**$43,963**
Average							**$4,396**

Note: Totals may not sum due to independent rounding.

Similarly, we use earlier estimates for the calculation of per-entity costs for drills and exercises, account security measures, multifactor authentication, cybersecurity training, penetration testing, vulnerability management and resilience.

For drills and exercises, we assume that a CySO on behalf of each owner and operator will develop cybersecurity components to add to existing physical security drills and exercises. This development is expected to take 0.5 hours for each of the 4 annual drills and 8 hours for an annual exercise. Using the loaded hourly wage for a CySO of $84.14, we estimate annual costs of approximately $841 per facility owner or operator [$84.14 CySO wage × ((0.5 hours × 4 drills) + (8 hours × 1 exercise)) = $841], as seen in

table 34.

For account security measures, we assume that a database administrator on behalf of each owner or operator will spend 8 hours each year implementing and managing account security. Using the loaded hourly wage for a database administrator of $71.96, we estimate annual costs of approximately $576 ($71.96 database administrator wage × 8 hours = $576), as seen in table 34.

For multifactor authentication, we assume that an owner or operator of a facility or OCS facility will spend $9,000 in the initial year on average to implement a multifactor authentication system and spend approximately $150 per employee annually for system maintenance and support. Therefore, we estimate first year costs of approximately $20,100 [$9,000 implementation cost + ($150 support and maintenance costs × 74 average facility company employees)], and subsequent year costs of $11,100 ($150 support and maintenance costs × 74 average facility company employees), as seen in table 34.

For cybersecurity training, we assume that a CySO will take 2 hours each year to develop and manage employee cybersecurity training, and employees at a facility or OCS facility will take 1 hour to complete the training each year. Using the estimated CySO wage of $84.14 and the estimated facility employee wage of $60.34, we estimate annual training costs of approximately $4,633 [($84.14 × 2 hours) + ($60.34 × 74 facility company employees × 1 hour)].

For penetration testing, we estimate costs only in the second and seventh years of analysis since tests are required to be performed in conjunction with submitting and renewing the Cybersecurity Plan. We assume that facility owners and operators will spend approximately $5,000 per penetration test and an additional $50 per IP address at the organization in order to capture network complexity. We use the total number of company employees as a proxy for the number of IP addresses, since the Coast Guard

does not have data on IP addresses or the network complexity at a given company. As a result, we estimate second- and seventh-year costs of approximately $8,700 [$5,000 testing cost + ($50 × 74 employees)], as seen in table 34.

For vulnerability management, we assume that each facility or OCS facility will need to secure a vulnerability scanning program or software. Because vulnerability scans can occur in the background, we do not assume an additional hour burden associated with the implementation or use of a vulnerability scanner each year. Using the annual subscription cost of an industry leading vulnerability scanning software, we estimate annual costs of approximately $3,390, as seen in table 34.

Finally, for resilience, we assume that each facility or OCS facility owner or operator will need to make at least one cybersecurity incident report per year. While this is incongruent with historical data that shows the entire affected population of facilities and OCS facilities reports only 18 cybersecurity incidents per year, we are attempting to capture a complete estimate of what the costs of this proposed rule could be for an affected entity. As such, we estimate that a CySO will need to take 0.15 hours to report a cybersecurity incident to the NRC, leading to annual per entity costs of approximately $13 ($84.14 CySO wage × 0.15 hours), as seen in table 34.

We perform the same calculations to estimate the per-entity costs for owners and operators of U.S.-flagged vessels. However, the estimates for the population of U.S.-flagged vessels have more dependency upon the type and number of vessels owned by the company being analyzed. This is largely due to the varying numbers of employees per vessel, by vessel type. We estimate fixed, average per-entity costs of approximately $10,877 per U.S.-flagged vessel owner or operator, as seen in table 36.

Table 36: Summary of Fixed Costs of the Proposed Rule per Owner or Operator of U.S.-flagged Vessels (2022 Dollars, 10-year Undiscounted Costs)[87]

Year	Cybersecurity Plan	Drills and Exercises	Account Security Measures	Multifactor Authentication	Cybersecurity Training	Penetration Testing	Vulnerability Management	Cyber Incident Reporting	Total
1	$3,366	$841	$576	$9,000	$168	$0	$3,390	$13	$17,354
2	$6,731	$841	$576	$0	$168	$5,000	$3,390	$13	$16,719
3	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
4	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
5	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
6	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
7	$1,515	$841	$576	$0	$168	$5,000	$3,390	$13	$11,503
8	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
9	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
10	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
Total									**$108,765**
Average									**$10,877**

Note: Totals may not sum due to independent rounding.

[87] The cost estimates in table 36 represent the costs incurred at a company level for each U.S.-flagged vessel owner and operator, and thus must be added to the costs calculated in table 38, which are dependent on the type and number of vessels owned, to create a full picture of the estimated costs per owner or operator. When these totals are multiplied over the full number of affected entities, the calculated totals will exceed those estimated for the population of U.S.-flagged vessels elsewhere in the analysis because we assume that each owner or operator will need to implement all cost-creating provisions of the proposed rule. This is discussed in further detail in the analysis of costs per owner or operator.

To estimate the per-entity costs that are dependent upon the number and type of vessel, we use the number of employees per vessel, and in the case of cybersecurity training costs, a unique weighted hourly wage based on the personnel employed on each vessel type as calculated in Appendix A: Wages Across Vessel Types. Table 37 displays the average number of employees for each vessel type, including shoreside employees, and their unique weighted mean hourly wages. Table 38 displays the per-vessel costs associated with each type of vessel.

Table 37: Summary of Employees and Wages by Vessel Type

Vessel Type	Number of Employees per Vessel (Includes Shoreside)	Weighted Mean Hourly Wage
MODU	372	$39.60
Subchapter I Vessels	82	$46.36
OSVs	16	$54.92
Subchapter H Passenger Vessels	85	$41.85
Subchapter K Passenger Vessels	35	$45.52
Subchapter M Towing Vessels	13	$51.28
Subchapter D and Combination Subchapters O&D Tank Vessels	40	$55.94
Subchapter D, O, or I Barges	0	$0.00
Subchapters K and T International Passenger Vessels	27	$44.59

Table 38: Summary of Annual Costs of the Proposed Rule per U.S.-flagged Vessels Based on Type of Vessel (2022 Dollars, Undiscounted Costs)

Vessel Type	Vessel Count	Multifactor Authentication	Cybersecurity Training	Penetration Testing (Years 2 and 7)[88]	Total
MODU	1	$55,800	$14,731	$18,600	$89,131
Subchapter I Vessels	1	$12,300	$3,802	$4,100	$20,202
OSVs	1	$2,400	$879	$800	$4,079
Subchapter H Passenger Vessels	1	$12,750	$3,557	$4,250	$20,557
Subchapter K Passenger Vessels	1	$5,250	$1,593	$1,750	$8,593
Subchapter M Towing Vessels	1	$1,950	$667	$650	$3,267

[88] When adding these costs to the fixed costs for owners and operators, only add these estimated penetration testing costs in years 2 and 7.

Subchapter D and Combination Subchapters O&D Tank Vessels	1	$6,000	$2,238	$2,000	$10,238
Subchapter D, O, or I Barges	1	$0	$0	$0	$0
Subchapters K and T International Passenger Vessels	1	$4,050	$1,204	$1,350	$6,604

In order to calculate the total cost per-entity in the population of U.S.-flagged vessels, we add the annual per-vessel costs from table 38 based on the number and types of vessels owned to the fixed costs estimated in table 36.

To estimate the cost for an owner or operator of a U.S.-flagged vessel to develop, resubmit, conduct annual maintenance, and audit the Cybersecurity Plan, we use estimates provided earlier in the analysis. The hour-burden estimates are 80 hours for developing the Cybersecurity Plan (average hour burden), 8 hours for annual maintenance of the Cybersecurity Plan (which would include amendments), 12 hours to renew Cybersecurity Plans every 5 years, and 40 hours to conduct annual audits of Cybersecurity Plans. Based on estimates from Coast Guard VSP reviewers at MSC, approximately 10 percent of Plans would need to be resubmitted in the second year due to revisions that would be needed to the Plans, which is consistent with the current resubmission rate for VSPs. For renewals of Plans after 5 years (occurring in the seventh year of the analysis period), Cybersecurity Plans would need to be further revised and resubmitted in approximately 10 percent of cases as well. However, in this portion of the analysis, we estimate costs as though the owner or operator will need to revise and resubmit their Plans in all cases resulting in an upper-bound (high) estimate of per-entity costs. We estimate the time for revision and resubmission to be about half the time to develop the Cybersecurity Plan itself, or 40 hours in the second year of submission, and 6 hours after 5 years (in the seventh year of the analysis period). Because we include the

annual Cybersecurity Assessment in the cost to develop Plans, and we do not assume that owners and operators will wait until the second year of analysis to begin developing the Cybersecurity Plan or implementing related cybersecurity measures, we divide the estimated 80 hours to develop Plans equally across the first and second years of analysis.

Using the CySO loaded hourly CySO wage of $84.14, we estimate the Cybersecurity Plan-related costs by adding the total number of hours to develop, resubmit, maintain, and audit each year and multiplying by the CySO wage. For example, we estimate owners and operators would incur approximately $6,731 in costs in year 2 of the analysis period [$84.14 CySO wage × (40 hours to develop the Plan + 40 hours to revise and resubmit the Plan) = $6,731]. See table 39.

Table 39: Cybersecurity Plan-Related Costs per Owner or Operator of a U.S.-flagged Vessel (2022 Dollars, 10-year Undiscounted Costs)

Year	CySO Wage	Hours to Develop Plan	Hours to Resubmit Plan	Annual Maintenance Hours	Audit Hours	Total
1	$84.14	40	0	0	0	$3,366
2	$84.14	40	40	0	0	$6,731
3	$84.14	0	0	8	40	$4,039
4	$84.14	0	0	8	40	$4,039
5	$84.14	0	0	8	40	$4,039
6	$84.14	0	0	8	40	$4,039
7	$84.14	12	6	0	0	$1,515
8	$84.14	0	0	8	40	$4,039
9	$84.14	0	0	8	40	$4,039
10	$84.14	0	0	8	40	$4,039
Total						**$39,885**
Average						**$3,989**

Note: Totals may not sum due to independent rounding.

Similarly, we use earlier estimates for the calculation of per-entity costs for drills and exercises, account security measures, multifactor authentication, cybersecurity training, penetration testing, vulnerability management, and resilience.

For drills and exercises, we assume that a CySO on behalf of each owner and operator will develop cybersecurity components to add to existing physical security drills

and exercises. This development is expected to take 0.5 hours for each of the 4 annual drills and 8 hours for an annual exercise. Using the loaded hourly wage for a CySO of $84.14, we estimate annual costs of approximately $841 per vessel owner or operator [$84.14 CySO wage × ((0.5 hours × 4 drills) + (8 hours × 1 exercise)) = $841], as seen in table 36.

For account security measures, we assume that a database administrator on behalf of each owner or operator will spend 8 hours each year implementing and managing account security. Using the loaded hourly wage for a database administrator of $71.96, we estimate annual costs of approximately $576 ($71.96 database administrator wage × 8 hours = $576), as seen in table 36.

For multifactor authentication, we assume that a vessel owner or operator will spend $9,000 in the initial year on average to implement a multifactor authentication system and spend approximately $150 per employee annually for system maintenance and support. Therefore, we estimate first year fixed costs of approximately $9,000 for all owners and operators, with annual costs in years 2 through 10 dependent on the number of employees for each type of vessel. For example, we estimate the first-year costs to an owner or operator of one OSV to be approximately $11,400 [$9,000 implementation cost + ($150 support and maintenance costs × 16 average employees per OSV)], and subsequent year costs of $2,400 ($150 support and maintenance costs × 16 average employees per OSV). Fixed per-entity implementation costs of $9,000 can be found in table 36, and variable per-vessel costs can be found in table 38.

For cybersecurity training, we assume that a CySO for each vessel owner or operator will take 2 hours each year to develop and manage employee cybersecurity training, and vessel employees will take 1 hour to complete the training each year. The per employee costs associated with training vary depending on the types and number of vessels and would be based on the average number of employees per vessel and the

associated weighted hourly wage. For example, using the estimated CySO wage of $84.14 and the estimated OSV employee wage of $54.91, we estimate annual training costs of approximately $1,047 [($84.14 × 2 hours) + ($54.91 × 16 average employees per OSV × 1 hour)]. Fixed per-entity costs of $168 can be found in table 36 and variable per-vessel costs can be found in table 38.

For penetration testing, we estimate costs only in the second and seventh years of analysis since tests are required to be performed in conjunction with submitting and renewing the Cybersecurity Plan. We assume that owners and operators of vessels will spend approximately $5,000 per penetration test and an additional $50 per IP address at the organization in order to capture network complexity. We use the average number of employees per vessel as a proxy for the number of IP addresses, since the Coast Guard does not have data on IP addresses or the network complexity at a given company. As a result, we estimate second- and seventh-year costs as follows: [$5,000 testing cost + ($50 × average number of employees per vessel)]. For example, we estimate second- and seventh-year cost of approximately $5,800 for an owner or operator of an OSV [$5,000 testing cost + ($50 × 16 average number of employees per OSV)]. Fixed per-entity costs of $5,000 can be found in table 36, and variable per-vessel costs can be found in table 38.

For vulnerability management, we assume that each U.S.-flagged vessel owner or operator will need to secure a vulnerability scanning program or software. Because vulnerability scans can occur in the background, we do not assume an additional hour burden associated with the implementation or use of a vulnerability scanner each year. Using the annual subscription cost of an industry leading vulnerability scanning software, we estimate annual costs of approximately $3,390, as seen in table 36.

Finally, for resilience, we assume that each U.S.-flagged vessel owner or operator will need to make at least one cybersecurity incident report per year. While this is incongruent with historical data that shows the entire affected population of vessels only

reports two cybersecurity incidents per year on average, we are attempting to capture a complete estimate of what the costs of the proposed rule could be for an affected entity. As such, we estimate that a CySO will need to take 0.15 hours to report a cybersecurity incident to the NRC, leading to annual per-entity costs of approximately $13 ($84.14 CySO wage × 0.15 hours), as seen in table 34.

Unquantifiable Cost Provisions or No-Cost Provisions of this Proposed Rule

Communications

Under proposed § 101.645, this NPRM would require CySOs to have a method to effectively notify owners and operators of facilities, OCS facilities, and U.S.-flagged vessels, as well as personnel of changes in cybersecurity conditions. The proposed requirements would allow effective and continuous communication between security personnel on board U.S.-flagged vessels and at facilities and OCS facilities; U.S.-flagged vessels interfacing with a facility or an OCS facility, the cognizant COTP, and national and local authorities with security responsibilities. Based on communication requirements established in 33 CFR 105.235 for facilities, 106.240 for OCS facilities, and 104.245 for vessels, the Coast Guard assumes that owners and operators of vessels, facilities, and OCS facilities already have communication channels established for physical security notifications which could easily be used for cybersecurity notifications. As a result, we do not estimate regulatory costs for communications. The Coast Guard requests public comment on this assumption and whether this communications provision would add an additional time burden.

Device Security Measures

Under proposed § 101.650(b)(1), this NPRM would require owners and operators of U.S. facilities, OCS facilities, and U.S.-flagged vessels to develop and maintain a list of company-approved hardware, firmware, and software that may be installed on IT or OT systems. This approved list would be documented in the Cybersecurity Plan.

Because this requirement would be included in the development of the Cybersecurity Plan, we estimated these costs earlier in that section of the cost analysis.

Under proposed § 101.650(b)(2), this NPRM would require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to ensure applications running executable code are disabled by default on critical IT and OT systems. Based on information from CGCYBER, the time it would take to disable such applications is likely minimal; however, we currently lack data on how prevalent these applications are within the affected population. Therefore, we are unable to estimate the regulatory costs of this proposed provision. The Coast Guard requests public comments on the device security measures under this regulatory provision.

Under proposed § 101.650(b)(3) and (4), this NPRM would require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to develop and maintain an accurate inventory of network-connected systems, the network map, and OT device configuration. Because these items would be developed and documented as a part of the Cybersecurity Plan, we previously estimated these costs in that section of the cost analysis.

Data Security Measures

Under proposed § 101.650(c), this NPRM would require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to securely capture, store, and protect data logs, as well as encrypt all data in transit and at rest. The Jones Walker survey (see footnote 69) reveals that 64 percent of U.S. facilities and OCS facilities are currently performing active data logging and retention, and 45 percent are always encrypting data for the purpose of communication.

Because data logging can be achieved with default virus-scanning tools, such as Windows Defender on Microsoft systems, the cost of storage and protection of data logs is primarily a function of the data space required to store them. Based on information

from CGCYBER, cloud storage can cost from $21 to $41 per month for 1 terabyte of data, $54 to $320 per month for 10 terabytes, and up to $402 to $3200 per month for 100 terabytes of data. However, the Coast Guard does not have information on the amount of data space the affected population would need to comply with this proposed rule, or if data purchases would be necessary in all cases. Therefore, we are unable to estimate regulatory costs for this proposed provision. The Coast Guard requests public comment on these estimates and any additional information on this proposed regulatory provision.

Similarly, encryption is often available in default systems, or in publicly available algorithms.[89] The Coast Guard would accept these encryption standards that came with the software or on default systems. However, there are potentially some IT and OT systems in use that do not have native encryption capabilities. In these instances, encryption would likely represent an additional cost. However, the Coast Guard does not have information on the number of systems lacking encryption capabilities. As a result, we are unable to estimate the regulatory costs for encryption above and beyond what is included in default systems, and we request public comment on the potential costs associated with this provision.

Supply Chain Management

Under proposed § 101.650(f)(1) and (2), this NPRM would include provisions to specify measures for managing supply chain risk. This would not create any additional hour burden, as owners and operators would only need to consider cybersecurity capabilities when selecting third-party vendors for IT and OT systems or services. In addition, based on information from CGCYBER, most third-party providers have existing cybersecurity capabilities and already have systems in place to notify the owners and operators of facilities, OCS facilities, and U.S.-flagged vessels of any cybersecurity

[89] For example, see the following webpages for descriptions of default encryption policies on Google and Microsoft programs and cloud-based storage systems: https://cloud.google.com/docs/security/encryption/default-encryption and https://learn.microsoft.com/en-us/microsoft-365/compliance/encryption?view=o365-worldwide, accessed July 19, 2023.

vulnerabilities, incidents, or breaches that take place. Therefore, the Coast Guard does not estimate a cost for this proposed provision.

Additionally, under proposed § 101.650(f)(3), this NPRM would require owners and operators of U.S. facilities, OCS facilities, and U.S.-flagged vessel to monitor third-party remote connections and document how and where a third party connects to their networks. Based on information from CGCYBER, many IT and OT vendors provide systems with the ability to remotely access the system to perform maintenance or trouble-shoot problems as part of a warranty or service contract. Because remote access is typically identified in warranties and service contracts, the Coast Guard assumes that industry is already aware of these types of connections and would only need to document them when developing the Cybersecurity Plan. We estimated these costs previously in the development of the Cybersecurity Plan section of this cost analysis. The Coast Guard requests public comment on the validity of this assumption and any additional information on this proposed regulatory provision.

Network Segmentation

Under proposed § 101.650(h)(1) and (2), this NPRM would require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to segment their IT and OT networks and log and monitor all connections between them. Based on information from CGCYBER, CG-CVC, and NMSAC, network segmentation can be particularly difficult in the MTS, largely due to the age of infrastructure in the affected population of facilities, OCS facilities and U.S.-flagged vessels. The older the infrastructure, the more challenging network segmentation may be. Given the amount of diversity and our uncertainty regarding the state of infrastructure across the various groups in our affected population, we are not able to estimate the regulatory costs associated with this proposed provision. The Coast Guard requests public comment on the anticipated costs of network

segmentation within the affected population, especially from those who have previously segmented networks at their organizations.

Physical Security

Under proposed § 101.650(i)(1) and (2), this NPRM would require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to limit physical access to IT and OT equipment; secure, monitor, and log all personnel access; and establish procedures for granting access on a by-exception basis. The Coast Guard assumes that owners and operators have already implemented physical access limitations and systems, by which access can be granted on a by-exception basis, based on requirements established in §§ 104.265 and 104.270 for vessels, §§ 105.255 and 105.260 for facilities, and §§ 106.260 and 106.265 for OCS facilities. Therefore, we do not believe that this proposed rule would impose new regulatory costs on owners and operators of facilities, OCS facilities, and U.S.-flagged vessels for this provision. However, we understand that § 101.650(i)(2), which requires potential blocking, disabling, or removing of unused physical access ports on IT and OT infrastructure, may represent taking steps above and beyond what has been expected under established requirements. The Coast Guard currently lacks information on the prevalence of these physical access ports on systems in use in the affected population, and therefore cannot currently calculate an associated cost. We request public comment on the anticipated costs associated with physical security provisions in this proposed rule above and beyond what has already been incurred under existing regulation.

Lastly, it is likely that this proposed rule would have unquantifiable costs associated with the incompatibility between the installation of the proposed newer software and the use of older or legacy software systems on board U.S.-flagged vessels, facilities, and OCS facilities. We request comments from the public on the anticipated

costs associated with this difference in software for the affected population of this proposed rule.

Sources of Uncertainty Related to Quantified Costs in the Proposed Rule

Given the large scope of this proposed rule, our analysis contains several areas of uncertainty that could lead us to overestimate or underestimate the quantified costs associated with certain provisions. In table 39, we outline the various sources of uncertainty, the expected impact on cost estimates due to the uncertainty, potential cost ranges, and a ranking of the source of uncertainty based on how much we believe it is impacting the accuracy of our estimates. A rank of 1 indicates that we believe the source of uncertainty has the potential to cause larger overestimates or underestimates than a source of uncertainty ranked 2, and so on. The Coast Guard requests public comment from members of the affected populations of facilities, OCS facilities, and U.S.-flagged vessels who could provide insight into the areas of uncertainty specified in table 40, especially those relating to potential cost estimates, hour burdens, or current baseline activities.

Table 40: Sources of Uncertainty in the Proposed Rule

Source of Uncertainty or Relevant Provision	Reason for Uncertainty	Impact on Cost Estimates	Potential Cost Range	Rank
Baseline cybersecurity activities in the U.S.-flagged vessel population	The Coast Guard was able to estimate current cybersecurity activity related to some of the proposed provisions in the population of facilities and OCS facilities based on the results of the "Ports and Terminals Cybersecurity Survey" conducted by Jones Walker. However, we lack similar information on current cybersecurity activity in the population of U.S.-flagged vessels, and instead assumed that affected vessel entities have no level of baseline activity. This has led to overestimated costs for the affected population of U.S.-flagged vessels.	Overestimate	N/A	1

Correction of vulnerabilities, performing fixes, and alleviating issues discovered in assessments, testing, or scanning	The proposed rule includes various types of provisions dealing with cybersecurity testing, assessment, and monitoring that are designed to help owners and operators identify vulnerabilities and other security issues that may be impacting an organization's IT and OT systems. While the provisions for cybersecurity measures of this proposed rule are designed to address many vulnerabilities that may be discovered, the Coast Guard has no way of calculating the costs associated with any fixes or mitigations that may be necessary above and beyond what is outlined in the proposed rule. The costs associated with mitigations and vulnerability corrections would be highly dependent on what is discovered and would vary from affected entity to affected entity, making cost estimates unreliable.	Underestimate	Not able to estimate.	2
Future cybersecurity technology upgrades	Many of the provisions for cybersecurity measures under proposed § 101.650 involve the implementation of hardware and software solutions to improve cybersecurity or monitor vulnerabilities within an organization's IT and OT systems. Because cybersecurity technology is rapidly evolving, we expect that upgrades to implemented solutions may be necessary in later years. However, the Coast Guard lacks information on how often or how costly these upgrades may be.	Underestimate	Not able to estimate.	3

§ 101.650(h)(1) and (2) - Network segmentation	Network segmentation can be particularly difficult in the MTS, largely due to the age of infrastructure in the affected population of facilities, OCS facilities and U.S.-flagged vessels. The older the infrastructure, the more challenging network segmentation may be. Given the amount of diversity and our uncertainty regarding the state of infrastructure across the various groups in our affected population, we are not able to estimate the regulatory costs associated with this proposed provision.	Underestimate	Not able to estimate.	4

§ 101.650(c) - Store data logs and encrypt data	Data logging can be achieved in the background using programs native to common computer operating systems, and therefore has a negligible cost. The primary cost would be the data space necessary to store the data logs. The Coast Guard does not currently know who in the affected population would need to purchase additional data space to store logs, if any. Similarly, the Coast Guard does not know who in the affected population would need to purchase data encryption capabilities given a lack of information on systems in use that lack encryption capabilities.	Underestimate	The costs would scale with the amount of data space purchased. Based on current market prices, cloud-based storage can cost from $21 to $41 per month for 1 terabyte of data, $54 to $320 per month for 10 terabytes, and up to $402 to $3200 per month for 100 terabytes of data.	5

§ 101.650(g)(4) - Perform and secure data backups	Backing up data can be achieved in the background using programs native to common computer operating systems, and therefore has a negligible cost. The primary cost would be the data space necessary to store the data logs. The Coast Guard does not currently know who in the affected population would need to purchase additional data space to store logs, if any. Similarly, the Coast Guard does not know who in the affected population would need to purchase data encryption capabilities or other security measures for data backups given a lack of information on systems in use that lack these capabilities.	Underestimate	The costs would scale with the amount of data space purchased. Based on current market prices, cloud-based storage can cost from $21 to $41 per month for 1 terabyte of data, $54 to $320 per month for 10 terabytes, and up to $402 to $3200 per month for 100 terabytes of data.	5
§ 101.650(i)(2) - Removable media and hardware	While the Coast Guard believes that limiting of physical access to critical IT and OT systems is likely already being done under existing regulation, requiring blocking, disabling, or removing of unused physical access ports on IT and OT infrastructure may represent efforts above and beyond requirements already in regulation. However, the Coast Guard currently lacks information on the prevalence of these physical access ports on systems in use in the affected population, and therefore cannot currently estimate an associated cost.	Underestimate	Costs could range from installing security or antitamper tape over unused USB or other access ports, installing access port locks, or taking the time to manually disable or remove ports from system hardware. Costs for antitamper tape typically range from approximately $10 to $20 per 55-yard roll. Costs for access port locks range from approximately $10 to $20 for a pack of 10	6

			locks. Costs for manually disabling ports on system hardware would be dependent on the time taken to disable, either through a software program or physically with a medium like caulk or epoxy resin. In either case, we estimate this would take approximately 1 to 5 minutes per access port.	
§ 101.650(b)(2) - Disable applications running executable code by default on critical IT and OT systems	The Coast Guard has limited data on what applications are prevalent in the affected population that may need to have executable code disabled.	Underestimate	Potential costs are likely negligible. The time required to disable these applications is likely small and only required to be performed once. Many operating systems include this policy by default, and it could be considered a no-cost provision of the proposed rule.	7

The uncertainty surrounding these aspects of this analysis makes estimating many costs challenging. The Coast Guard has considered several alternative scenarios to demonstrate how alternative assumptions may affect the cost estimates presented in this analysis.

First, we consider an alternative assumption regarding the baseline cybersecurity activities in the population of U.S.-flagged vessels, which we determined may have the biggest impact on our cost estimates for this proposed rule. Because the Coast Guard lacks data on current cybersecurity activities in the population of U.S.-flagged vessels, we assume that all owners and operators of U.S.-flagged vessels have no baseline cybersecurity activity to avoid potentially underestimating costs in the preceding cost analysis. However, we were able to use existing survey data to estimate baseline cybersecurity activity in the population of facilities and OCS facilities, which allowed us to more accurately estimate the cost impacts of many of the proposed provisions.

If we use the same rates of baseline activity we assume for facilities and OCS facilities for the U.S.-flagged vessels as well, we would see a reduction in undiscounted cost estimates related to account security measures, multifactor authentication implementation and management, cybersecurity training, and penetration testing. Like the rates of baseline activity cited for the population of facilities and OCS facilities, this alternative would assume that 87 percent of the U.S.-flagged vessel population are managing account security, 83 percent have implemented multifactor authentication, 25 percent are conducting cybersecurity training, and 68 percent are conducting penetration tests.[90] Using these assumptions would result in estimated annual population costs of approximately $119,891 for account security ($922,239 primary estimated cost × 0.13), $5,670,537 for multifactor authentication implementation and maintenance ($33,356,100 primary estimated cost × 0.17), $4,827,371 for cybersecurity training ($6,436,494

[90] See footnote 69.

primary estimate cost × 0.75), and $4,583,264 for penetration testing ($14,322,700 primary estimated cost × 0.32). This would result in reduced undiscounted annual cost estimates of approximately $47,882,654 for the population of U.S.-flagged vessels. See table 41.

Table 41: Comparison of Primary and Alternative Cost Estimates for U.S.-flagged Vessel Population (2022 Dollars, Undiscounted Costs)

Source of Cost	Primary Cost Estimates	Alternative Estimates
Account Security Costs	$922,239	$119,891
Multifactor Authentication Costs	$33,356,100	$4,336,293
Cybersecurity Training Costs	$6,436,494	$836,744
Penetration Testing Costs	$14,322,700	$1,861,951
Total	**$55,037,533**	**$7,154,879**

The Coast Guard requests comment on whether these assumptions of baseline activity are more reasonable than what is currently used in this RIA, or if there are additional alternative assumptions about baseline activities in these areas or other areas not discussed that would lead to more accurate estimates.

In addition, we considered adding cost estimates for those areas of uncertainty where we were able to estimate a range of potential costs. For proposed provisions in § 101.650(c) and (g) related to storing data logs and performing data backups, we anticipate that this data storage will be set up to occur in the background, meaning systems will not need to be taken offline and no burden hours. However, this makes the associated cost a function of the data space required to store and backup data. While we do not have information on how much data space a given company would need, we can estimate industry costs based on SME estimates for a range of potential data space amounts. As described in table 40, current market prices indicate that cloud-based storage can cost from $21 to $41 per month for 1 terabyte of data, $54 to $320 per month for 10 terabytes, and up to $402 to $3200 per month for 100 terabytes of data. To

estimate the annual cost of 1 additional terabyte of data, we take the average estimated monthly cost of $31 [($41 + $21) ÷ 2] and multiply it by 12 to find the average annual cost of $372 per terabyte. If each facility and OCS facility company required an additional terabyte of data space as a result of this proposed rule, we would estimate approximately $635,376 ($372 × 1,708 facility owners and operators) in additional undiscounted annual costs to industry. Similarly, if we assumed each U.S.-flagged vessel company required an additional terabyte of data space because of this proposed rule, we would estimate approximately $660,300 ($372 × 1,775 vessel owners and operators) in additional undiscounted annual costs to industry. See table 42.

Table 42. Comparison of Alternative Data Space Cost Estimates for the Affected Population and Impact on Undiscounted Cost Totals (2022 Dollars, Undiscounted Costs)

Affected Population	Annual Data Space Cost Estimates	Total Data Space Cost Estimates Over 10 Years	Primary Population Cost Totals Over 10 Years	Alternative Population Cost Totals Over 10 Years
Facilities and OCS Facilities	$635,376	$6,353,760	$312,330,251	$318,684,011
U.S.-flagged Vessels	$660,300	$6,603,000	$439,884,727	$446,487,727
Total	**$1,295,676**	**$12,956,760**	**$752,214,978**	**$765,171,738**

These costs could change if we were to add additional assumptions about current baseline activities or adjusted the expected need for data space. Therefore, we request public comment on the accuracy and inclusion of these estimates.

Government Costs

There are three primary drivers of Government costs associated with this proposed rule. The first would be under proposed § 101.630(e), where owners and operators of the affected population of U.S.-flagged vessels, facilities, and OCS facilities would be required to submit a copy of their Cybersecurity Plan for review and approval to either the cognizant COTP or the OCMI for facilities or OCS facilities, or to the MSC for U.S.-flagged vessels. In addition, proposed § 101.630(f) would require owners and

operators to submit Cybersecurity Plan amendments to the Coast Guard, under certain conditions, for review and approval. The second cost driver is related to the marginal increase in inspection time as a result of added Cybersecurity Plan components that will be reviewed as a part of an on-site inspection of facilities, OCS facilities, and U.S.-flagged vessels. The final cost driver would be under proposed § 101.650(g)(1), where owners and operators of the affected population of U.S.-flagged vessels, facilities, and OCS facilities would be required to report cyber incidents to the NRC. The NRC would then need to process the report and generate notifications for each incident report they receive. The Coast Guard examines these costs under the assumption that we will use the existing frameworks in place to review security plans and amendments, process incident reports, and conduct inspections. Given uncertainty surrounding Coast Guard staffing needs related to this proposed rule, we have not estimated costs associated with new hires or the establishment of a centralized office.

First, we analyze the costs to the Government associated with reviewing and approving Cybersecurity Plans and amendments. Based on Coast Guard local facility inspector estimates, it would take plan reviewers about 40 hours to review an initial Cybersecurity Plan for a facility or OCS facility, 8 hours to review a resubmission of a Plan in the initial year, and 4 hours to review an amendment in years 3 through 6 and 8 through 10 of the analysis period. It would also take about 8 hours of review for the renewal of plans in year 7 of the analysis period, and another 8 hours for any necessary resubmissions of Plan renewals. The hour-burden and frequency estimates for resubmissions and amendments are consistent with estimates for resubmissions of FSPs and OCS FSPs, as we expect the Cybersecurity Plans and amendments to be of a similar size and scope. As discussed earlier in the analysis, we estimate that resubmissions of initial Cybersecurity Plans and Plan renewals occur at a rate of 10 percent in years 2 and

7 of the analysis period. We use the number of facilities and OCS facilities that would submit Plans, which would be about 3,411.

We determine the wage of a local facility inspector using publicly available data found in Commandant Instruction 7310.1W.[91] We use an annual mean hourly wage rate of $89 for an inspector at the O-3 (Lieutenant) level, based on the occupational labor category used in ICR 1625-0077.

We estimate the undiscounted second-year (initial year of Plan review) cost for the Coast Guard to review Cybersecurity Plans for U.S. facilities and OCS facilities to be approximately $12,385,952 [(3,411 facility Plan initial submissions × $89.00 × 40 hours) + (341 facility Plan resubmissions × $89.00 × 8 hours)]. Except in year 7, when renewal of all Plans would occur, we estimate the undiscounted annual cost to the Coast Guard for the review of amendments to be approximately $1,214,316 (3,411 amendments × $89.00 × 4 hours). In year 7, we estimate the undiscounted cost to be approximately $2,671,424 [(3,411 Plans for 5-year renewal × $89.00 × 8 hours) + (341 facility Plan resubmissions × $89.00 × 8 hours)]. We estimate the discounted cost for the Coast Guard to review facility and OCS facility Cybersecurity Plans to be approximately $18,059,127 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $2,571,213, using a 7-percent discount rate. See table 43.

[91] Readers can view Commandant Instruction 7310.1W for military personnel at media.defense.gov/2022/Aug/24/2003063079/-1/-1/0/CI_7310_1W.PDF, accessed January 2024.

Table 43: Estimated Government Costs of Proposed Rule for Facility and OCS Facility Cybersecurity Plan and Amendment Review (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rate)

Year	Reviewer Wage	Facility Cybersecurity Plan Submissions	Facility Cybersecurity Resubmissions	Cybersecurity Plan Review Hours	Resubmission Review Hours	Amendment Review Hours	Total Cost	7%	3%
1	$89.00	0	0	0	0	0	$0	$0	$0
2	$89.00	3411	341	40	8	0	$12,385,952	$10,818,370	$11,674,948
3	$89.00	3411	0	0	0	4	$1,214,316	$991,244	$1,111,271
4	$89.00	3411	0	0	0	4	$1,214,316	$926,396	$1,078,904
5	$89.00	3411	0	0	0	4	$1,214,316	$865,791	$1,047,480
6	$89.00	3411	0	0	0	4	$1,214,316	$809,150	$1,016,971
7	$89.00	3411	341	8	8	0	$2,671,424	$1,663,629	$2,172,112
8	$89.00	3411	0	0	0	4	$1,214,316	$706,743	$958,592
9	$89.00	3411	0	0	0	4	$1,214,316	$660,507	$930,672
10	$89.00	3411	0	0	0	4	$1,214,316	$617,297	$903,565
Total							**$23,557,588**	**$18,059,127**	**$20,894,515**
Annualized							**$2,355,759**	**$2,571,213**	**$2,449,475**

Note: Totals may not sum due to independent rounding.

Based on Coast Guard MSC estimates, it would take about 28 hours to review an initial U.S.-flagged vessel Cybersecurity Plan, 8 hours to review a resubmission of the Cybersecurity Plan in the initial year, and 4 hours to review an amendment in years 3 through 6 and 8 through 10 of the analysis period. It would also take about 8 hours of review for the renewal of Plans, and another 8 hours to review resubmitted Plan renewals in year 7 of the analysis period. The hour-burden and frequency estimates for resubmissions and amendments are consistent with estimates for resubmissions of VSPs, as we expect the Cybersecurity Plans and amendments to be of a similar size and scope. We use the number of U.S.-flagged vessel owners and operators who would submit Plans, about 1,775.

According to ICR 1625-0077, the collection of information related to VSPs, FSPs, and OCS FSPs, the MSC uses contract labor to conduct Plan and amendment reviews. The MSC provided us with its independent Government cost estimate for their existing contract for VSP reviews. The average loaded annual mean hourly wage rate for the various contracted reviewers from the independent Government cost estimate is $81.83.

We estimate the undiscounted second-year cost for the Coast Guard to review Cybersecurity Plans for U.S.-flagged vessels to be approximately $4,183,477 [(1,775 initial vessel Plan submissions × $81.83 × 28 hours) + (178 vessel Plan resubmissions × $81.83 × 8 hours)]. Except in year 7, when resubmission of all Plans would occur, we estimate the undiscounted annual cost to the Coast Guard for reviewing amendments to be approximately $580,993 (1,775 amendments × $81.83 × 4 hours). In year 7, we estimate the undiscounted cost to be approximately $1,278,512 [(1,775 Plans for 5-year renewal × $81.83 × 8 hours) + (178 facility Plan resubmissions × $81.83 × 8 hours)]. We estimate the discounted cost for the Coast Guard to review U.S.-flagged vessel Cybersecurity Plans to be approximately $7,118,596 over a 10-year period of analysis,

using a 7-percent discount rate. We estimate the annualized cost to be approximately $1,013,528, using a 7-percent discount rate. See table 44.

Table 44: Estimated Government Costs of U.S.-Flagged Vessel Cybersecurity Plan and Amendment Review (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rate)

Year	Reviewer Wage	Vessel Cybersecurity Plan Submissions	Vessel Cybersecurity Plan Resubmissions	Cybersecurity Plan Review Hours	Resubmission Review Hours	Amendment Review Hours	Total Cost	7%	3%
1	$81.83	0	0	0	0	0	$0	$0	$0
2	$81.83	1775	178	28	8	0	$4,183,477	$3,654,011	$3,943,328
3	$81.83	1775	0	0	0	4	$580,993	$474,263	$531,691
4	$81.83	1775	0	0	0	4	$580,993	$443,237	$516,205
5	$81.83	1775	0	0	0	4	$580,993	$414,240	$501,170
6	$81.83	1775	0	0	0	4	$580,993	$387,140	$486,572
7	$81.83	1775	178	8	8	0	$1,278,512	$796,193	$1,039,547
8	$81.83	1775	0	0	0	4	$580,993	$338,143	$458,641
9	$81.83	1775	0	0	0	4	$580,993	$316,022	$445,283
10	$81.83	1775	0	0	0	4	$580,993	$295,347	$432,313
Total							**$9,528,940**	**$7,118,596**	**$8,354,750**
Annualized							**$952,894**	**$1,013,528**	**$979,432**

Note: Totals may not sum due to independent rounding.

The second source of Government costs would be the marginal increase in onsite inspection time due to the expansion of FSPs, OCS FSPs, and VSPs to include the Cybersecurity Plans and provisions proposed by this NPRM. The proposed cybersecurity provisions would add to the expected onsite inspection times for the populations of facilities, OCS facilities, and U.S.-flagged vessels. Coast Guard SMEs within CG-FAC conferred with local inspection offices to estimate the expected marginal increase in facility and OCS facility inspection time. Local facility inspectors estimate that the additional cybersecurity provisions from this proposed rule would add an average of 1 hour to an onsite inspection, and that the inspection would typically be performed by an inspector at a rank of O-2 (Lieutenant Junior Grade). According to Commandant Instruction 7310.1W Reimbursable Standard Rates, an inspector with an O-2 rank has a fully loaded wage rate of $72.[92] Therefore, we estimate the annual undiscounted Government cost associated with the expected marginal increase in onsite inspections of facilities and OCS facilities is $245,592 (3411 facilities and OCS facilities × 1 hour inspection time × $72 facility inspector wage). We estimate the total discounted cost of increased inspection time to be approximately $1,724,936 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $245,592, using a 7-percent discount rate. See table 45.

Table 45: Estimated On-site Inspection of Facilities and OCS Facilities Costs for Government of the Proposed Rule (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Facilities	Facility Inspection Hours	Facility Inspector Wage	Total Cost	7 Percent	3 Percent
1	3411	1	$72	$245,592	$229,525	$238,439
2	3411	1	$72	$245,592	$214,510	$231,494
3	3411	1	$72	$245,592	$200,476	$224,751
4	3411	1	$72	$245,592	$187,361	$218,205
5	3411	1	$72	$245,592	$175,104	$211,850
6	3411	1	$72	$245,592	$163,648	$205,679

[92] Readers can view Commandant Instruction 7310.1W for military personnel at media.defense.gov/2022/Aug/24/2003063079/-1/-1/0/CI_7310_1W.PDF, accessed December 2023.

7	3411	1	$72	$245,592	$152,942	$199,689
8	3411	1	$72	$245,592	$142,937	$193,873
9	3411	1	$72	$245,592	$133,586	$188,226
10	3411	1	$72	$245,592	$124,847	$182,744
Total				**$2,455,920**	**$1,724,936**	**$2,094,950**
Annualized				**$245,592**	**$245,592**	**$245,592**

Note: Totals may not sum due to independent rounding.

Similarly, Coast Guard SMEs within CG-ENG estimate that the additional cybersecurity provisions from the proposed rule would add an average of 0.167 hours (10 minutes) to an on-site inspection of a U.S.-flagged vessel and that the inspection would typically be performed by an inspector at a rank of E-5 (Petty Officer Second Class). According to Commandant Instruction 7310.1W Reimbursable Standard Rates, an inspector with an E-5 rank has a fully loaded wage rate of $58. Therefore, we estimate the annual undiscounted Government cost associated with the expected marginal increase in onsite inspections of U.S.-flagged vessels is $99,630(10,286 vessels × 0.167 hours inspection time × $58 facility inspector wage). We estimate the total discounted cost of increased inspection time to be approximately $699,761 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $99,630, using a 7-percent discount rate. See table 46.

Table 46: Estimated On-site Inspection of U.S.-flagged Vessels Costs for Government of the Proposed Rule (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Vessels	Vessel Inspection Hours	Vessel Inspector Wage	Total Cost	7 Percent	3 Percent
1	10286	0.167	$58	$99,630	$93,112	$96,728
2	10286	0.167	$58	$99,630	$87,021	$93,911
3	10286	0.167	$58	$99,630	$81,328	$91,176
4	10286	0.167	$58	$99,630	$76,007	$88,520
5	10286	0.167	$58	$99,630	$71,035	$85,942
6	10286	0.167	$58	$99,630	$66,388	$83,439
7	10286	0.167	$58	$99,630	$62,045	$81,008
8	10286	0.167	$58	$99,630	$57,986	$78,649
9	10286	0.167	$58	$99,630	$54,192	$76,358
10	10286	0.167	$58	$99,630	$50,647	$74,134

Total				**$996,300**	**$699,761**	**$849,865**
Annualized				**$99,630**	**$99,630**	**$99,630**

Note: Totals may not sum due to independent rounding.

The final source of Government costs from this proposed rule would be the time to process and generate notifications for each cyber incident reported to the NRC. As discussed earlier in our analysis of costs associated with cyber incident reporting, from 2018 to 2022, the NRC fielded and processed an average of 18 cyber incident reports from facilities and OCS facilities, and an average of 2 cyber incident reports from U.S.-flagged vessels, for a total of 20 cyber incident reports per year. In addition, the NRC generated an average of 31 notifications for appropriate Federal, State, local and tribal agencies per processed cyber incident over that same time period, meaning an average of 620 notifications per year (20 cyber incident reports × 31 notifications).

Based on ICR 1625-0096, Report of Oil or Hazardous Substance Discharge; and Report of Suspicious Maritime Activity, it takes the NRC approximately 0.15 hours (8.5 minutes) to receive an incident report, and 0.2 hours (12 minutes) to disseminate a verbal notification to the Federal on-scene coordinator or appropriate Federal agency. Given that cyber incidents and the reports of suspicious activity detailed in the ICR are processed in a similar fashion, we use the same hour estimates here. According to ICR 1625-0096, a contractor, equivalent to a GS-9, processes incident reports and generates relevant notifications. We use the GS-9-Step 5 hourly basic rate from the Office of Personnel Management (OPM) 2022 pay table, or $29.72.[93] To account for the value of benefits to government employees, we first calculate the share of total compensation of Federal employees accounted for by wages. The Congressional Budget Office (2017) reports total compensation to Federal employees with a bachelor's degree (consistent

[93] Please see: https://www.opm.gov/policy-data-oversight/pay-leave/salaries-wages/salary-tables/pdf/2022/RUS_h.pdf. We use the Rest of U.S. (RUS) rate here to maintain consistency with the rates used in ICR 1612-0096; accessed July 12, 2023.

with a GS level of GS-7 to GS-10) as $67.00 per hour and associated wages as $39.50.[94] This implies that total compensation is approximately 1.70 times the average wage ($67.00 ÷ $39.50). Therefore, we can calculate $50.52 ($29.72 × 1.70 load factor) as the fully loaded wage rate for the NRC contractor equivalent to a GS-9, Step 5.

We estimate undiscounted annual Government costs of cyber incident report processing and notification to be $6,416 [(20 cyber incident reports × 0.15 hours to process × $50.52 contractor wage) + (620 notifications × 0.2 hours × $50.52 contractor wage)]. We estimate the total discounted cost to be approximately $45,064 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $6,416, using a 7-percent discount rate. See table 47.

Table 47: Estimated Government Costs of Cyber Incident Report Processing (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Number of Incidents Processed	Hours to Process	Number of Notifications Generated	Hours to Generate Notification	NRC Wage	Total Cost	7%	3%
1	20	0.15	620	0.2	$50.52	$6,416	$5,996	$6,229
2	20	0.15	620	0.2	$50.52	$6,416	$5,604	$6,048
3	20	0.15	620	0.2	$50.52	$6,416	$5,237	$5,872
4	20	0.15	620	0.2	$50.52	$6,416	$4,895	$5,701
5	20	0.15	620	0.2	$50.52	$6,416	$4,575	$5,534
6	20	0.15	620	0.2	$50.52	$6,416	$4,275	$5,373
7	20	0.15	620	0.2	$50.52	$6,416	$3,996	$5,217
8	20	0.15	620	0.2	$50.52	$6,416	$3,734	$5,065
9	20	0.15	620	0.2	$50.52	$6,416	$3,490	$4,917
10	20	0.15	620	0.2	$50.52	$6,416	$3,262	$4,774
Total						**$64,160**	**$45,064**	**$54,730**
Annualized						**$6,416**	**$6,416**	**$6,416**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted Government costs of the proposed rule for the review of Cybersecurity Plans, increase in on-site inspection time, and processing cyber incident reports to be approximately $27,647,481 over a 10-year period of analysis, using

[94] Congressional Budget Office (2017), "Comparing the Compensation of Federal and Private-Sector Employees, 2011 to 2015," https://www.cbo.gov/system/files/115th-congress-2017-2018/reports/52637-federalprivatepay.pdf, accessed July 19, 2023.

a 7-percent discount rate. We estimate the annualized cost to be approximately $3,936,379, using a 7-percent discount rate. See table 48.

Table 48: Total Estimated Government Costs of the Proposed Rule (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facility Cyber Plan Review Costs	Vessel Cyber Plan Review Costs	Facility Inspection Costs	Vessel Inspection Costs	Incident Report Processing and Notification Costs	Total Cost	7 Percent	3 Percent
1	$0	$0	$245,592	$99,630	$6,416	$351,638	$328,634	$341,396
2	$12,385,952	$4,183,477	$245,592	$99,630	$6,416	$16,921,067	$14,779,515	$15,949,729
3	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,752,548	$1,964,761
4	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,637,896	$1,907,535
5	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,530,744	$1,851,975
6	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,430,601	$1,798,034
7	$2,671,424	$1,278,512	$245,592	$99,630	$6,416	$4,301,574	$2,678,804	$3,497,573
8	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,249,543	$1,694,820
9	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,167,797	$1,645,456
10	$1,214,316	$580,993	$245,592	$99,630	$6,416	$2,146,947	$1,091,399	$1,597,530
Total						**$36,602,908**	**$27,647,481**	**$32,248,809**
Annualized						**$3,660,291**	**$3,936,379**	**$3,780,544**

Note: Totals may not sum due to independent rounding.

Total Costs of the Proposed Rule

We estimate the total discounted costs of the proposed rule to industry and government to be approximately $562,740,969 over a 10-year period of analysis, using a 7-percent discount rate. We estimate the annualized cost to be approximately $80,121,654, using a 7-percent discount rate. See table 49.

Table 49: Total Estimated Costs of the Proposed Rule to Industry and Government (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facility and OCS Facility Costs	U.S.-flagged Vessel Costs	Government Costs	Total Costs	7 Percent	3 Percent
1	$33,469,773	$53,613,063	$351,638	$87,434,474	$81,714,462	$84,887,839
2	$37,053,260	$54,116,840	$16,921,067	$108,091,167	$94,411,011	$101,886,292
3	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$59,913,465	$67,168,260
4	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$55,993,893	$65,211,903
5	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$52,330,741	$63,312,527
6	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$48,907,234	$61,468,473
7	$25,788,807	$49,425,867	$4,301,574	$79,516,248	$49,518,723	$64,653,986
8	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$42,717,473	$57,939,931
9	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$39,922,872	$56,252,360

10	$30,859,773	$40,389,851	$2,146,947	$73,396,571	$37,311,095	$54,613,942
Total	**$312,330,251**	**$439,884,727**	**$36,602,908**	**$788,817,886**	**$562,740,969**	**$677,395,513**
Annualized				**$78,881,789**	**$80,121,654**	**$79,411,419**

Note: Totals may not sum due to independent rounding.

Benefits

Malicious cyber actors, including individuals, groups, and nation states, have rapidly increased in sophistication over the years and use techniques that make them more and more difficult to detect. Recent years have seen the rise of cybercrime as a service, where malicious cyber actors are hired to conduct cyber-attacks.[95] Some national governments have also used ransomware to advance their strategic interests, including evading sanctions.[96] The increased growth of cybercrime is a factor that has intensified in the last 20 years. Per the Federal Bureau of Investigation's cybercrime reporting unit, financial losses from reported incidents of cybercrime exceeded $10.3 billion in 2022, and $35.9 billion since 2001.[97] While there are significant private economic incentives for MTS participants to implement their own cybersecurity measures, and survey results indicate that MTS participants are more confident in their cybersecurity capabilities than in years past, the same survey indicates that there are important gaps in capabilities that leave the MTS and downstream economic participants exposed to risk.[98] In the 2018 report, the CEA stated, "[b]ecause no single entity faces the full costs of the adverse cyber events, the Government can step in to achieve the optimal level of cybersecurity,

---

[95] See https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world/ for a description of cybercrime as a service and https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ for a description of its growth in recent years. Accessed December 6, 2023.

[96] Institute for Security and Technology, "RTF Report: Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force," https://securityandtechnology.org/ransomwaretaskforce/report/, accessed July 19, 2023.

[97] See the Federal Bureau of Investigation's "2022 Internet Crime Report," Internet Crime Complaint Center (IC3), March 14, 2023. This report can be found at https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, accessed December 4, 2023. For a summary of financial losses from reported incidents of cybercrime since 2001, see https://www.statista.com/statistics/267132/total-damage-caused-by-by-cybercrime-in-the-us/, accessed December 4, 2023.

[98] Readers can access the survey in the docket or at https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html; accessed July 19, 2023. See page 16 of the survey for data on industry confidence and pages 34 - 41 for data on cybersecurity practices.

either through direct involvement in cybersecurity or by incentivizing private firms to increase cyber protection."[99]

The overall benefit of this proposed rule would be the reduced risk of a cyber incident and, if an incident occurs, improved mitigation of its impact. This would benefit owners and operators and help protect the maritime industry and the United States. We expect this proposed rule would have significant but currently unquantifiable benefits for the owners and operators of facilities, OCS facilities, and U.S.-flagged vessels, as well as downstream economic participants[100] and the public at large. This proposed rule would benefit the owners and operators of facilities, OCS facilities, and U.S.-flagged vessels by having a means, through the Cybersecurity Plan, to ensure that all cybersecurity measures are in place and tested periodically, which would improve the resiliency of owners and operators to respond to a cyber incident and to maintain a current cybersecurity posture, reducing the risk of economic losses for owners and operators as well as downstream economic participants. For example, this proposed rule would require training, drills, and exercises, which would benefit owners and operators by having a workforce that is knowledgeable and trained in most aspects of cybersecurity, which reduces the risk of a cyber incident and mitigates the impact if an incident occurs. Conducting training, drills, and exercises would also enable the owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to prevent, detect, and respond to a cyber incident with improved capabilities.

In addition, cybersecurity measures in this proposed rule would require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to identify weaknesses or vulnerabilities in their IT and OT systems and to develop strategies or safeguards to identify and detect security breaches when they occur. The software and

---

[99] Economic Report of the President *supra* note 1 at 369.

[100] Downstream economic participants are entities or individuals involved in the later stages of the supply chain or production process, such as distributors, wholesalers, service providers, and retailers that supply and sell products directly to consumers.

physical requirements of this proposed rule would ensure that there is the minimal level of protection for critical IT and OT systems and allow for the proper monitoring of these systems. In table 50, we list the expected benefits associated with each major regulatory provision of the proposed rule.

Table 50. Expected Actions of the Proposed Rule that Accrue Benefits

§ 101.630 Cybersecurity Plan	1. Improved incident response: A well-designed Cybersecurity Plan includes procedures for incident response and enables vessels and port facilities to address cybersecurity incidents quickly and effectively to minimize their impact and duration. 2. Employee awareness and training: A Cybersecurity Plan includes employee training and awareness programs, which ensures that staff members (1) understand their role in protecting both the vessel and port facility's digital assets to prevent cyber incidents, and (2) know how to respond to potential threats to minimize their impact and duration.
§ 101.635 Drills and Exercises	1. Increased awareness and understanding: Cybersecurity drills and exercises promote a better understanding of the risks and challenges associated with cyber threats among all stakeholders, including crew members, port facility personnel, and other relevant parties, allowing them to better prevent cyber incidents. 2. Improved preparedness: Regular drills and exercises help organizations to identify vulnerabilities in their cybersecurity posture, allowing them to develop and implement effective countermeasures to address potential threats and prevent cyber incidents. 3. Enhanced response capabilities: Drills and exercises allow staff to practice their roles and responsibilities during a potential cybersecurity incident, ensuring they can respond quickly and effectively to minimize the impact of any potential cyber-attacks. 4. Identification of gaps and weaknesses: By simulating real-world cyber-attacks, organizations can identify gaps in their security policies, procedures, and technologies, and take appropriate steps to address gaps in those areas to prevent cyber incidents. 5. Continuous improvement: Regularly conducting drills and exercises allows organizations to learn from their experiences and refine and update their Cybersecurity Plans and strategies to ensure ongoing effectiveness in preventing cyber incidents.
§ 101.645 Communications	1. Improved situational awareness: Clear communication enables stakeholders to stay

	informed about potential cyber threats and vulnerabilities, allowing them to respond promptly and effectively. 2. Enhanced collaboration: Effective communication fosters collaboration between different departments, stakeholders, and external partners, such as shipping companies, port authorities, and cybersecurity experts. This collaboration is crucial for identifying and mitigating cybersecurity risks. 3. Streamlined incident response: In the event of a cyber-attack or security breach, effective communication helps ensure that all relevant parties are aware of the situation and can coordinate their response efforts, minimizing the impact of the incident.
§ 101.650 Cybersecurity Measures. (a) *Account security measures*.	1. Preventing unauthorized use: A secured account prevents malicious actors from using it as a platform to spread malware, spam, or launch other attacks, ensuring systems remain operational and free from disruption. 2. Preserving digital identity: Prevents cyber criminals from using compromised accounts to impersonate the account holder, reducing identity theft or other fraudulent activities. This promotes trust in clients and partners and maintains the positive reputation of the organization in the marketplace. 3. Personal data protection: Accounts often contain or provide access to personal and sensitive information. Securing them ensures this data remains confidential and prevents it from being stolen, altered, or deleted. Further, the organizations can promote greater consumer confidence by protecting client data from malicious actors. 4. Maintaining privacy: Securing accounts helps in safeguarding private communications, photos, videos, and other personal content from unauthorized access and prevents it from being stolen, altered, or deleted, retaining the trust of clients and partners.
§ 101.650 Cybersecurity Measures. (b) *Device security measures*.	1. Limiting spread: Secured devices can prevent malware or malicious activities from spreading to other connected devices or networks, mitigating the effects of a cyber incident. 2. Data protection: Prevent unauthorized access, theft, or damage to personally identifiable information (PII) and other sensitive data. This includes financial information, health records, intellectual property, and other confidential data. By protecting the digital assets of the organization and its clients, organizations can help prevent their customers from becoming unwitting victims of cybercrime and

	lessen the impacts of cyber incidents on other economic participants, increasing consumer trust and commerce in the U.S. economy. 3. Reduced vulnerability: Regularly updated and secured devices are less vulnerable to the newest exploits or zero-day attacks, reducing the chance of cyber-attacks and mitigating the effects of a cyber incident. 4. Limiting spread: Secured devices can prevent malware or malicious activities from spreading to other connected devices or networks, mitigating the effects of a cyber incident.
§ 101.650 Cybersecurity Measures. (c) *Data security measures*.	1. Protecting sensitive information: Both vessels and port facilities handle sensitive data, such as personal information from crew and passengers, cargo details, financial transactions, and operational data. Data security measures help protect this information from unauthorized access, ensuring privacy and compliance with regulations for data protection. This measure helps prevent sensitive data from being stolen, altered, or deleted. Thus, the organization retains the trust of clients and partners and helps protect downstream economic participants from the effects of a cyber incident. 2. Building trust and reputation: Ensuring sensitive information remains secure and maintaining reliable operations contribute to a positive reputation for shipping companies and port facilities. This can lead to increased business opportunities, better relationships with stakeholders, and improved trust of clients and partners. 3. Promoting collaboration and information sharing subject to any applicable antitrust limitations: Secure data sharing between vessels, port facilities, and other stakeholders in the maritime industry is essential for effective collaboration and coordination, which helps facilitate early warnings about cyber threats and incidents to improve response times and mitigate impacts to other actors. Also, collective data and lessons learned can be used to develop better security practices and policies, helps determine the "appropriate levels of defense investments," and facilitate the "effective functioning of the cyber insurance market."[101] Data security measures help create an environment where parties can confidently share information without compromising its confidentiality, integrity, or availability. In its 2018 report, the CEA stated, "Government-monitored information-sharing platforms for anonymous disclosures of adverse

[101] Economic Report of the President *supra* note 1 at 370.

	cyber events are designed to increase the real-time awareness of cyber vulnerabilities and facilitate timely and publicly shared security solutions." The CEA also states that "the Government can be a valuable contributor to sharing threat information."[102]
§ 101.650 Cybersecurity Measures. (d) *Cybersecurity training for personnel*.	1. Enhanced security awareness: Cybersecurity training increases awareness of potential threats, vulnerabilities, and best practices, empowering personnel to take a proactive approach to addressing potential cyber risks and preventing cyber incidents. 2. Risk reduction: Training helps reduce the risk of successful cyber-attacks by teaching personnel how to identify, mitigate, and respond to threats; thus, reducing the potential for costly disruptions to maritime operations. 3. Improved incident response: Training equips personnel with the skills necessary to effectively respond to and recover from cyber incidents, which minimizes damage and downtime. 4. Strengthened collaboration and communication: Cybersecurity training fosters a culture of shared responsibility among all stakeholders, encouraging collaboration and communication between onboard and port facility personnel, as well as with other entities in the maritime industry, which helps prevent cyber incidents. 5. Continuous improvement: Regular cybersecurity training helps to keep personnel updated on the latest threats, technologies, and best practices, ensuring that maritime cybersecurity measures remain effective at preventing cyber incidents over time. 6. Reduction in human error: Cybersecurity training helps reduce the likelihood of human errors, such as falling victim to phishing attacks or accidentally exposing sensitive information, which are some of the most common causes of security incidents. This prevents an accidental cyber incident or falling victim to cyber-attacks such as a phishing attack.
§ 101.650 Cybersecurity Measures. (e) *Risk management*.	1. Protection of critical assets: By managing cybersecurity risks, ship and port facilities can better protect essential assets such as navigation systems, communication systems, cargo handling equipment, and access control systems from cyber threats, preventing disruptions to the system and maintaining business continuity. 2. Strengthened resilience: Developing a comprehensive CRM plan enables vessels and port facilities to respond to and recover from cyber

[102] Economic Report of the President *supra* note 1 at 370 and 327.

	incidents more quickly, mitigating the impact of an attack and recovering quickly from cyber-attacks.
§ 101.650 Cybersecurity Measures. (f) *Supply chain*.	1. Reduced risk of cyber-attacks: By ensuring that hardware and software components are genuine, untampered, and up to date, a secure supply chain helps to minimize vulnerabilities that can be exploited by cyber-attackers. Organizations with a secure supply chain can assure partners and customers of the reliability and safety of their goods and services. The benefit of avoiding supply chain disruptions may be the reduction in the "spillover effects to economically linked firms" and possibly a reduction in risk to "corporate partners, employees, customers, and firms with a similar business model."[103] Multiple authentication methods "may help prevent cyber breaches across the supply chain,"[104] thereby reducing the cost of incidents when they occur. 2. Enhanced trust: A secure supply chain promotes trust among stakeholders, such as customers, partners, and regulatory agencies, by demonstrating a commitment to maintaining high cybersecurity standards. Organizations with a secure supply chain are better equipped to deal with disruptions, ensuring smooth operations and uninterrupted supply chain processes for their business partners, which maintains their Organization's share of the commerce. 3. Better risk management: A comprehensive understanding of supply chain security risks allows organizations to develop effective risk management strategies, reducing the likelihood of cyber-attacks and their potential impact.
§ 101.650 Cybersecurity Measures. (g) *Resilience*.	1. Protection of sensitive data: Cyber resilience helps protect sensitive information, such as customer data, intellectual property, and trade secrets, from being stolen or compromised by hackers. Cyber resilience is about minimizing the financial losses associated with data breaches, ransomware, and other cyber threats. In its 2018 report, the CEA stated from a case study that a data breach of PII "will likely negatively affect the firm's ability to raise new capital and make new investments" and generally may adversely affect a firm's stock price.[105] Therefore, protecting sensitive information may be beneficial in protecting a firm's market value. 2. Business continuity: A cyber-resilient organization can maintain or quickly resume operations in the

[103] Economic Report of the President *supra* note 1 at 362.
[104] Economic Report of the President *supra* note 1 at 382-383.
[105] Economic Report of the President *supra* note 1 at 342.

	event of a cyber-attack, minimizing downtime and ensuring that essential services remain available to customers and stakeholders. 3. Reputation and trust: A strong cyber resilience posture can enhance an organization's reputation and foster trust with customers, partners, and stakeholders, as it demonstrates a commitment to protecting their data and interests.
§ 101.650 Cybersecurity Measures. (h) *Network segmentation*.	1. Enhanced security: By segregating the network into separate segments, each with its own access controls, network segmentation helps to minimize the risk of unauthorized access to critical systems and sensitive data. This reduces the potential for cyber-attacks, data breaches, and other security incidents. It also reduces disruptions to operations and the impact of the cyber incident, and, thereby, economic losses to firms. 2. Easier monitoring and management: Segmented networks can be more easily monitored and managed. Administrators can more effectively track network traffic and troubleshoot issues, as well as apply and enforce security policies on a per-segment basis, preventing cyber incidents. 3. Isolating issues: If a security breach or a technical problem occurs within one network segment, it can be more easily contained, preventing the issue from spreading throughout the entire network. This can minimize the impact on operations and reduce the time and resources required to address the issue.
§ 101.650 Cybersecurity Measures. (i) *Physical security*.	1. Prevention of unauthorized access: Physical security measures can prevent unauthorized individuals from accessing sensitive areas or equipment, such as data centers, server rooms, or computer systems, where critical information is stored. Direct access to critical assets like servers, computers, and storage devices can cause immediate and significant damage. For example, destruction of physical assets can be a greater financial burden and more difficult to recover from after an attack, and the loss or destruction of PII, loss of financial data, and online services being down during the attack may result in lost revenues. 2. Protection of hardware: Implementing physical security measures can protect valuable hardware and equipment from theft, tampering, or damage. This includes devices like servers, workstations, routers, switches, and storage devices. Physical security represents a first line of defense against an internal attack. Direct access would enable the attackers to bypass digital security measures like firewalls or encryption, directly impacting core systems and data. Protecting hardware may help prevent against the

	loss or destruction of PII, loss of financial data, lost revenue, and so on. 3. Deterrent to attackers: Visible physical security measures can deter potential attackers and make it more difficult for them to execute a cyber-attack. This can include security cameras, access control systems, or security personnel. Physical damage to infrastructure can take longer to recover from, be more costly, and is potentially irreversible. 4. Minimize the risk of insider threats: Physical security measures can help detect and prevent insider threats, such as employees or contractors attempting to access sensitive information or systems without authorization. Unlike digital breaches that often leave digital traces, physical breaches that are carried out by employees or contractors may go unnoticed until significant damage has occurred. Insider attacks can lead to loss of trust among customers, business partners, and stakeholders which could reduce the flow of commerce.

Cyber Incidents and Risks addressed by the Proposed Rule

In May 2021, the Colonial Pipeline Company suffered a cyber-attack that disrupted the supply of fuel to the east coast of the United States. Colonial Pipeline Company was forced to shut down operations for 6 days, which created gasoline and fuel shortages. In addition to the direct financial losses incurred by Colonial Pipeline Company, the shutdown and subsequent shortages negatively impacted consumers, creating a 4 cents-per-gallon increase in average gasoline prices in the impacted areas, with price increases lingering even after the pipeline returned to operation.[106] Further, fuel shortages caused some fuel stations to temporarily close due to shortened supply, and some airlines in the impacted area were forced to scramble for additional fuel sources and added additional stops along select long-haul flights.[107] This was a ransomware cyber-attack that, based on public reports, was a result of the attackers using a legacy Virtual

[106] Tsvetanov, T., & Slaria, S. (2021). The effect of the colonial pipeline shutdown on gasoline prices. Economics Letters, 209. https://doi.org/10.1016/j.econlet.2021.110122. Accessed December 14, 2023.
[107] Josephs, L. (2021). *Pipeline outage forces American Airlines to add stops to some long-haul flights, southwest flies in Fuel*. CNBC. https://www.cnbc.com/2021/05/10/colonial-pipeline-shutdown-forces-airlines-to-consider-other-ways-to-get-fuel.html, accessed January 18, 2024.

Private Network and Colonial Pipeline not having a two-factor authentication method, more commonly known as multifactor authentication, in place on its computer systems.[108] Therefore, it was possible for computer hackers to access Colonial Pipeline's computer systems with only a password. This proposed rule would likely prevent an attack similar to the Colonial Pipeline attack from occurring by requiring owners and operators of vessels, facilities, and OCS facilities to implement account security measures and multifactor authentication on their computer systems. An example of multifactor authentication would be requiring a five- or six-digit passcode after a password has been entered by company personnel. Multifactor authentication is part of account security measures in the proposed § 101.650.

The encryption of data in the proposed § 101.650 under data security measures may have relegated stolen data to being useless in the event of a cyber-attack. Furthermore, Colonial Pipeline would likely have benefitted from a penetration test, which they had not conducted, to ensure the safety and security of its critical systems. The proposed requirement of a penetration test would simulate real-world cyber-attacks that would help companies identify the risks to their computer systems and prepare the necessary measures to lessen the severity of a cyber-attack.

Additionally, under proposed § 101.650 for device security measures, documenting and identifying the network map and OT device configuration information, Colonial Pipeline may have been able to detect exactly where the connections to the affected systems were and may have been able to isolate the problem without having to shut down all pipeline operations, as it did temporarily, which greatly affected its fuel supply operations.

---

[108] U.S. Senate, Joseph Blount, Jr. Committee on Homeland Security & Governmental Affairs. "Hearing Before the United States Senate Committee on Homeland Security and Governmental Affairs - Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack." June 8, 2021. Washington, DC and via video conference. Text can be downloaded at https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack/, accessed June 28, 2023.

Lastly, Colonial Pipeline did not have a Cybersecurity Plan in place but did have an emergency response plan. With proposed §§ 101.630, Cybersecurity Plan, and 101.635, Drills and Exercises, a Cybersecurity Plan could have benefitted Colonial Pipeline because it includes periodic training and exercises that increase the awareness of potential cyber threats and vulnerabilities throughout the organization. A Cybersecurity Plan also creates best practices so company personnel have the knowledge and skills to identify, mitigate, and respond to cyber threats when they occur. Creating the Cybersecurity Plan would allow the CySO to ensure all aspects of the Plan have been implemented at a CySO's respective company. Improved awareness of potential cybersecurity vulnerabilities and the steps taken to correct them could have helped Colonial Pipeline identify its password weakness issue before it was exploited.

In another cyber-attack that occurred in 2017 against the global shipping company Maersk, computer hackers, based on public reports, exploited Maersk's computer systems because of vulnerabilities in Microsoft's Windows operating system. The malware was disguised as ransomware, which created more damage to Maersk's computer systems. In 2016, one year prior to the attack, IT professionals at Maersk highlighted imperfect patching policies, the use of outdated operating systems, and a lack of network segmentation as the largest holes in the company's cybersecurity. While there were plans to implement measures to address these concerns, they were not undertaken, leaving Maersk exposed and underprepared for the attack it faced in 2017. The effects of this attack were far-reaching. Beyond the direct financial losses incurred by Maersk (estimated at nearly $300 million), shipping delays and supply chain disruptions caused additional downstream economic losses that are much more difficult to quantify as shipments went unfulfilled for businesses and consumers, and trucks were forced to sit

and wait at ports.[109] Under proposed § 101.650, cybersecurity measures such as patching would likely prevent a similar attack from occurring and help prevent such losses. Patching vessel, facility, and OCS facility computer systems would ensure they are not vulnerable to a cyber-attack because the latest software updates would be installed on these systems with periodic software patches.

Additionally, penetration testing may have identified the vulnerabilities in Maersk's computer systems. Regular cybersecurity drills and exercises may have enabled Maersk's employees to quickly identify the cyber threat and may have reduced the impact and longevity of the cyber-attack. Further, network segmentation as proposed in § 101.650(h) could have helped stop the spread of malware to all its computer systems, which ultimately crippled its operations. By separating networks, Maersk could have better isolated the attack and kept larger portions of its business open, meaning fewer financial losses and downstream economic impacts to other companies and consumers.

Resilience played a significant role in Maersk's ability to recover from the cyber-attack quickly. Company personnel worked constantly to recover the affected data and eventually restored the data after 2 weeks.[110] Proposed § 101.650 contains provisions for resilience, which owners and operators such as Maersk must possess to recover from a cyber-attack. However, with proper backups of critical IT and OT systems, Maersk may have been able to recover more quickly from the attack.

The Coast Guard emphasizes that this proposed rule might also have quantifiable benefits from reducing or preventing lost productivity from a cyber incident and possibly

---

[109] Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"; *WIRED*; August 22, 2018; https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, accessed June 28, 2023.

[110] News reports suggest this recovery time was luck and not due to existing cybersecurity practices. "Maersk staffers finally found one pristine backup in their Ghana office. By a stroke of luck, a blackout had knocked the server offline prior to the NotPetya attack, disconnecting it from the network. It contained a single clean copy of the company's domain controller data, and its discovery was a source of great relief to the recovery team." See Daniel E. Capano, "Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk," September 30, 2021, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/, accessed July 25, 2023.

lost revenues from the time that critical IT and OT systems are inoperable as a result of a cyber incident, if one occurs. Such benefits would accrue to owners and operators of vessels and facilities, as well as to downstream participants in related commerce, and to the public at large. For instance, short-term disruptions to the MTS could result in increases to commodity prices, while prolonged disruptions could lead to widespread supply chain shortages. Short- and long-term disruptions and delays may affect other domestic critical infrastructure and industries, such as our national defense system, that depend on materials transported via the MTS.

The societal impacts from a cyber security incident such as the attack that occurred against Maersk are difficult to quantify. They may include the effects of delays in cargo being delivered, which could result in the loss of some or all of the cargo, especially if the cargo is comprised of perishable items such as food or raw goods, such as certain types of oil that would be later used in the supply chain to manufacture final goods such as food items. Delays themselves may result in the unfulfillment of shipping orders to customers as vessels wait offshore to enter a port, which would have the downstream effect of customers not receiving goods because delivery trucks would sit idle at ports until OT and IT systems either at the port or onboard vessels once again become operational after the attack. Other societal impacts could include, but are not limited to, delays in shipments of medical supplies that may be carried onboard vessels that would not be delivered on time to individuals and medical institutions who rely on these supplies for their healthcare needs and service, respectively. Therefore, it should be noted that a cyber-attack may have considerable economic impacts on multiple industries in the United States such as, but not limited to, healthcare, food, transportation, utilities, defense, and retail. It should also be noted that the Coast Guard is not able to estimate, quantify, or predict the societal harm of shipping delays from a cyber-attack on the MTS or the economic impact it could cause because it would be dependent on many variables

such as: the type of attack, the severity of the attack, the length of the attack, the response by the affected parties to the attack, and other variables.

The benefits of this NPRM could be particularly salient in the case of a coordinated attack by a malicious actor seeking to disrupt critical infrastructure for broader purposes. For instance, in a circumstance where the rule's provisions prevented a terrorist or nation-state actor[111] from using a cyber-attack in connection with a broader scheme that threatened human life, a strategic waterway, or a major port, the avoided economic and social costs may be substantial.

With respect to the latter, as noted by Cass R. Sunstein in *Laws of Fear: Beyond the Precautionary Principle (The Seeley Lectures, Series Number 6)*, "fear is a real social cost, and it is likely to lead to other social costs."[112] In addition, Ackerman and Heinzerling state "terrorism 'works' through the fear and demoralization caused by uncontrollable uncertainty." As devastating as the direct impacts of a successful cyber-attack can be on the U.S. marine transportation system and supply chain, avoiding the impacts of the more difficult to measure indirect effects of fear and demoralization in connection with a coordinated attack would also entail substantial benefits. However, the Coast Guard is not able to quantify these potential benefits because they would depend on the incident, the duration of the incident, and how various private and public actors would respond to the incident.

---

[111] For instance, the Office of the Director of National Intelligence recently reported on the cyber espionage and attack threats from multiple nation-states with respect to U.S. critical infrastructure. *See* Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community at 10, 15, 19 (Feb. 6, 2023), available at https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf (last visited July 31, 2023) (describing cyber threats associated with China, Russia, and Iran). A recent multi-national cybersecurity advisory noted that "Russian state-sponsored cyber actors have demonstrated capabilities to compromise IT networks; develop mechanisms to maintain long-term, persistent access to IT networks; exfiltrate sensitive data from IT and [OT] networks; and disrupt critical [ICS/OT] functions by deploying destructive malware." *See* Joint Cybersecurity Advisory, Russian State Sponsored and Criminal Cyber Threat to Critical Infrastructure, Alert AA22-110A (April 20, 2022), available at: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (accessed December 14, 2023).

[112] Cass R. Sunstein, *Laws of Fear*, at 127; Cambridge University Press (2005).

Through the provisions of this proposed rule, benefits from implementing and enhancing a cybersecurity program may likely increase over time. By requiring that a range of cybersecurity measures be implemented, such as account security measures, vulnerability scanning, and automated backups, an organization can drastically reduce the downtime it takes to remedy a breach. Education and training can also help guide employees to identify potential email phishing scams, suspect links, and other criminal efforts, which will likely increase protection against external and internal threats before they occur. Further, because so many of the proposed provisions include periodic updates and modifications following tests or assessments, we believe that cybersecurity programs will continue to improve each time they are tested and reexamined by the implementing entity.

This NPRM proposes to address the challenges facing businesses today by requiring the implementation of safeguards to cybersecurity on the MTS. In adopting these measures, owners and operators of U.S.-flagged vessels, facilities, and OCS facilities can take preemptive action before malicious actors and the threats they pose take advantage of vulnerabilities in their critical IT and OT systems.

Breakeven Analysis

While the Coast Guard is able to describe the qualitative benefits that this proposed rule may have for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities, and others who would be affected by a cyber-attack, the Coast Guard is not able to quantify and monetize benefits. One reason is that it is challenging to project the number of cyber-attacks that would occur over a relevant period without this proposed rule; another reason is that it is challenging to quantify the magnitude of the harm from such attacks. It is further challenging to quantify the marginal impact of this rulemaking, both because the Coast Guard cannot quantify the effectiveness of the provisions included in the proposals (how many attacks would be prevented or how much

damage would be mitigated) and because the Coast Guard has uncertainty around the appropriate baseline to consider regarding what cybersecurity actions are being taken for reasons beyond this rulemaking. Without such projections and quantification, it is not possible to monetize the benefits of the proposed rule in terms of harms averted. As an alternative, we present a breakeven analysis for this proposed rule.

Thus, this breakeven analysis only considers the $80 million in costs (at a 7 percent discount rate) that Coast Guard was able to quantify. The Coast Guard notes that, based on available data, there are likely additional costs the Coast Guard is not able to monetize. Furthermore, the downstream costs and impacts resulting from a cyber-attack on an individual firm are challenging to quantify given the overlapping and intersecting nature of the supply chain. However, research examining the overall impacts of the NotPetya cyber-attack (one of the largest cyber-attacks in history), estimates societal impacts and downstream costs nearly four times greater than the direct impact on the firm suffering the initial attack.[113] The Coast Guard requests comment on this finding and its relevance to the impact of cyber-attacks in the maritime transportation system specifically. To the extent that the costs of this proposed rule are higher than the Coast Guard's monetized estimate, the amount of costs this proposed rule must prevent would also need to increase to justify this proposed rule. The proposed rule would set the minimum requirements for companies to address their cybersecurity posture and provides the flexibility for these companies to take the necessary action to protect themselves from a cyber-attack.

OMB's Circular A-4 (September 17, 2003) states that, in the case of "non-quantified factors," agencies may consider the use of a threshold ("breakeven")

[113] For example, analysis of the NotPetya attack revealed overall estimates of impacts on customers four times greater than those on the firms directly impacted by the attack. For more details, please see: Matteo Crosignani et al, "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains," Federal Reserve Bank of New York Staff Reports, No. 937 (July 2020, revised July 2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf, accessed July 7, 2023.

analysis.[114] A breakeven analysis provides calculations to show how small or large the value of the non-quantified benefits could be before the proposed rule would yield zero net benefits. For this proposed rule, we calculate breakeven results from one example, using the estimated cost of a real-world cyber-attack on a regulated entity. Global shipper Maersk reported that it suffered an estimated $300 million in business costs and income losses due to a cyber-attack.[115] The actual losses were likely much larger than the $300 million in business impacts to Maersk due to impacts on Maersk's customers. Over the past decade, there have been numerous cyber-attacks—not just on the international and domestic maritime sector, but on other sectors of the U.S. and global economies.[116] In a paper published by Akpan, Bendiab, Shiaelis, Karamperidis, and Michaloliakos (2022), the authors state that the maritime sector has shown a 900-percent increase in cybersecurity breaches as it enters the digital era.[117] The paper adds that many automated systems on vessels, by their nature, are vulnerable to a cyber-attack, and include navigation systems such as Electronic Chart Display and Information Systems, Global Positioning Systems, and Global Navigation Satellite Systems. Other affected systems include radar systems; Automatic Identification Systems; communication systems; and systems that control the main engine, generators, among others (Akpan et al., 2022).[118] Furthermore, the paper presents the vulnerabilities and consequences of cyber-attacks to ships' systems ranging from hijacking ships, destroying and stealing

---

[114] Readers can access OMB Circular A-4 dated September 17, 2003, at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A4/a-4.pdf, accessed July 20, 2023.
[115] Greenberg, *supra* note 109.
[116] NIST provides a definition for the term "cyber-attack." Readers can access this definition at https://csrc.nist.gov/glossary/term/cyber_attack; accessed July 20, 2023.
[117] Frank Akpan, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis, and Michalis Michaloliakos; "Cybersecurity Challenges in the Maritime Sector"; *Network*; March 7, 2022; page 123; https://www.mdpi.com/2673-8732/2/1/9/pdf?version=1646653034; accessed May 2023. MDPI has open access to journals and published papers. Additionally, NIST provides a definition of the term *breach*, although not specifically related to cybersecurity at, https://csrc.nist.gov/glossary/term/breach, accessed July 2023.
[118] Akpan et al., *supra* note 117, at 129-30.

data, damaging equipment, disrupting vessel operations, uploading malware to computer systems, losing lives and cargo, and more (Akpan et al., 2022).[119]

In a paper by Jones (2016), the author noted that outdated systems are vulnerable to cyber-attacks.[120] The paper refers to a study that states 37 percent of servers running Microsoft failed to download the correct patch and left systems vulnerable to a cyber-attack. Additionally, Jones states that "many ships were built before cyber security was a major concern" and goes on to state that many newer software systems are not compatible with older software systems.

Akpan, et al. (2022) also list a few cyber-attacks that have occurred in the maritime transportation sector in the past few years. Allianz Global Corporate and Specialty (AGCS) reports that there was a record 623 million ransomware attacks in 2021.[121] In a paper published by Meland, Bernsmed, Wille, Rodseth, and Nesheim (2021), the authors state that 46 successful[122] cyber-attacks with a significant impact on the maritime industry have occurred worldwide between 2010 and 2020, or an average of 4.2 attacks a year.[123] Of the 46 attacks, the most notable cyber-attack stated by the authors of this paper, and earlier in the **Benefits** discussion of this preamble, occurred in 2017 against the shipping company Maersk. Maersk estimated their economic loss to be

---

[119] Id.

[120] Kevin Jones, "Threats and Impacts in Maritime Cyber Security," April 15, 2016, pages 7 and 8, https://pearl.plymouth.ac.uk/handle/10026.1/4387?show=full; accessed May 22, 2023.

[121] AGCS is a global insurance company. Readers can access this report at https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2022-press.html. The Coast Guard accessed this report in May 2023. AGCS's website is, https://www.agcs.allianz.com.

[122] The analysis did not include mere attempts to attack, unsuccessful attacks, or attacks categorized as "white hat" attacks, which are attempts to infiltrate cybersecurity systems to identify vulnerabilities in software, hardware, or networks. Definition of "white hat hacking" at https://www.fortinet.com/resources/cyberglossary/whitehat-security, accessed July 20, 2023.

[123] The title of this paper is "A Retrospective Analysis of Maritime Cyber Security Incidents." Readers can access this paper at https://www.semanticscholar.org/paper/A-Retrospective-Analysis-of-Maritime-Cyber-Security-Meland-Bernsmed/6caba4635f991dd1d99ed98cf640812f8cae16ba (pages 519 and 523). The Coast Guard accessed this pdf link in May 2023. Readers may need to create an account to view this paper, other papers, and research literature. The paper is also available at, https://www.transnav.eu. The authors of the study noted that shipping is a very diverse sector and that their source materials tend to focus on larger ships and operations. The authors stated that it is highly unlikely that this study has captured all the different cyber incidents over the sector. Additionally, the authors did not define what a "significant impact" entails; nevertheless, in some cyber-attacks they cited, they provided the effect of an attack in their description of the incident.

nearly $300 million in the form of costs and reduced income to a specific firm as the result of the incident (Meland et al., 2021). Based on other reports, the economic damage that resulted from this incident may have been considerably more because of the downstream impacts that this incident may have had on customers and other companies who rely on the shipping industry for their businesses.[124]

Monetizing the impact of the cyber-attack on Maersk allows the Coast Guard to create a breakeven point as it relates to a specific company (risk reduction percentage and the number of years the proposed rule would have to prevent one incident annually) for this proposed rule using the estimated costs of a cyber-attack that occurred against a shipping company. The breakeven point would be higher if effects on third parties were considered.

Although this cyber-attack did not occur against a U.S. company, and represents one attack against a single company, it impacted a large shipping company and affected almost one-fifth of global shipping operations, according to Meland, et al. (2021). The Coast Guard is using this incident as an example while understanding that the economic impact of a cyber-attack can vary greatly, depending upon the severity of a cyber-attack and the surrounding conditions. We acknowledge that the Maersk incident we use in this breakeven analysis may not be representative of other cyber-attacks that occur in the future in the maritime sector. Meland, et al. (2021), also state that a majority of cyber-attacks in the maritime industry were not reported.

---

[124] This figure does not include indirect effects on third parties, such as logistics firms and others who may have experienced losses because of this incident. See, for example, Matteo Crosignani et al, "Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains," Federal Reserve Bank of New York Staff Reports, No. 937 (July 2020, revised July 2021), https://www.newyorkfed.org/medialibrary/media/research/staff_reports/sr937.pdf, accessed July 7, 2023 (analyzing a sample of customers indirectly affected by the NotPetya attack, and concluding that "the customers of these directly hit firms [of the NotPetya attack] recorded significantly lower profits relative to similar but unaffected firms," with one measure of effects on customers being four times higher, in the aggregate, than effects on firms directly affected by the attack); Andy Greenberg, *Wired Magazine*, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" (August 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, accessed July 7, 2023 (describing indirect costs to logistics firms and other costs associated with a large-scale disruption to the global supply chain).

Using this example of a cyber-attack with our explanation in the benefits section of the RIA of how we believe this proposed rule may prevent such an attack, we can estimate a breakeven point. We take the estimated annualized[125] cost of this proposed rule using a 7-percent discount rate ($80.1 million)—which may be an underestimation of the actual costs that this proposed rule may impose on industry—and divide by the avoided loss from the Maersk attack ($300 million)—a loss that this proposed rule may prevent noting that the reported business loss of the Maersk attack may be an underestimate of the actual impact of the attack on social welfare.[126] From there, we obtain an annual risk-reduction value to the affected firm of approximately 0.267, or about 27 percent ($80.1 million ÷ $300 million), which is the minimum annual risk-reduction percentage that would need to occur to justify this proposed rule to the affected firm. If we state this another way, this proposed rule would need to reduce the risk or the likelihood of one or more successful cyber-attacks, similar to this attack, by approximately 27 percent annually for the benefits to justify the estimated costs to the affected firm. To be clear, the Coast Guard does not have an estimate for how much this proposed rule would actually reduce the risk of successful cyber-attacks on the MTS.

The Coast Guard estimates the number of years the proposed rule would have to prevent a cyber-attack to break even, though the Coast Guard cautions that it does not know the degree to which the proposed rule would prevent cyber-attacks. For an incident similar to the Maersk cyber-attack, we estimate this proposed rule would have to prevent at least one attack of this type (with the same avoided losses) approximately every 3.75 years ($300 million ÷ $80.1 million) to break even. Additionally, the losses from similar cyber-attacks may be lower given that this proposed rule may have the intended effect of

---

[125] We use annualized costs because we assume this proposed rule would result in constant reduced probability in every year following this proposed rule's implementation. Stated differently, we assume the risk reduction to be constant each year.

[126] The loss estimate used for the Maersk attack also represents a potential underestimation as it does not include indirect effects on third parties, such as logistics firms and others who may have experienced losses because of this incident. See footnote 113.

mitigating the size of losses from these types of attacks. Readers should also note that the losses estimated from this incident were reported by Maersk and not from an independent source. Table 51 summarizes the breakeven results of this NPRM.

Table 51. Summary of Breakeven Results of Proposed Rule

Breakeven Example	Annualized Cost of Proposed Rule (7% discount rate)	Avoided Losses	Required Risk Reduction	Required Frequency of Averted Cyber-attacks
Calculations	*a*	*b*	$c = a \div b$	$d = b \div a$
Maersk Attack	$80.1 million	$300 million (single-event loss)	0.267	One every 3.75 years

Analysis of Alternatives

Cybersecurity has become a critical issue across all sectors. The maritime industry, a pivotal component of the global supply chain, is no exception. With an increasing amount of sensitive data being stored and processed online, regulations are needed to protect this data from unauthorized access and breaches. As cyber threats grow more sophisticated and pervasive, it has become increasingly apparent that clear and actionable cybersecurity regulations are needed for the maritime industry. Furthermore, cybersecurity is not just a matter of individual or business concerns, it is also a national security issue. Robust regulations help protect critical infrastructure and government services from cyber-attacks that could threaten national stability. For instance, unauthorized access to a ship's navigation system could lead to disastrous consequences, including collisions or groundings, which can put people at risk and lead to economic losses for the affected entities and the U.S. economy. To prevent incidents like this, the Coast Guard has included several proposed regulatory provisions that identify potential network and system vulnerabilities. Of these provisions, penetration testing is one of the more intensive and costly, but would provide important benefits, including demonstrating where and how malicious actors could exploit system weaknesses, so that organizations can better prioritize cybersecurity upgrades and improvements based on risk.

Given the relatively high costs associated with penetration testing, and the significant vulnerability risks associated with not performing these tests, the Coast Guard contemplated four alternatives: (1) maintain the status quo; (2) require annual penetration testing and submission of results to the Coast Guard; (3) allow penetration testing at the discretion of the owner or operator; or (4) require penetration testing every 5 years in conjunction with the submission and approval of Cybersecurity Plans (the preferred alternative).

(1) Status quo

Currently. the Coast Guard does not require owners and operators of facilities, OCS facilities, and U.S.-flagged vessels to conduct penetration tests as a part of their security plans. Despite this, survey data indicates that some MTS entities are already conducting penetration tests for their organizations as they face an evolving cyber threat landscape. While we expect the adoption of penetration testing policies to grow over time, 32 percent of facility and OCS facility owners and operators (see footnote number 69) and an unknown number of U.S.-flagged vessel owners and operators have yet to add this test to their suite of cybersecurity measures.

Maintaining the status quo by not requiring any penetration testing would reduce the costs for affected owners and operators of the proposed rule by $28,549,669, with an annualized cost reduction of $4,064,831 over a 10-year period of analysis, discounted at 7 percent, when compared to the preferred alternative. However, not requiring penetration testing would leave a significant gap in the vulnerability detection capability of a large portion of the MTS, exposing MTS stakeholders and the wider U.S. economy to greater risk. Without periodic penetration tests to determine weaknesses in critical IT and OT systems, the affected population puts itself at greater risk of cyber incidents, which can endanger employees, consumers, and the supply chain. As a result, the Coast Guard rejected the status quo alternative and has proposed requiring penetration tests every 5

years, aligned with the renewal of a Cybersecurity Plan, as discussed in alternative (4), below.

(2) Annual Penetration Testing

Penetration testing represents a crucial element of a comprehensive cybersecurity strategy. It involves proactively testing computer systems, networks, and software applications to identify vulnerabilities that might be exploited by attackers. Because penetration testing provides a much more in-depth review of the vulnerabilities and weaknesses of IT and OT systems, the Coast Guard considered an alternative that would require it on an annual basis. Through annual penetration testing, an organization would be better equipped to identify weaknesses within their systems and prepare for real cyber threats. However, the costs and resources needed for penetration testing can be significant. As such, annual testing might impose an undue burden on the affected organizations.

Based on Coast Guard estimates, penetration testing would cost approximately $5,000 per test, plus an additional $50 per IP address at the organization to capture network complexity. By increasing the frequency of these tests, the costs to facilities, OCS facilities, and U.S. flagged vessels would increase significantly. Under the preferred alternative, which requires penetration testing every 5 years in conjunction with the submission and renewal of a Cybersecurity Plan, the Coast Guard estimates total costs of penetration testing to industry of $28,549,669 and annualized costs of $4,064,831 over a 10-year period of analysis, discounted at 7 percent (see the *Penetration Testing* section of the RIA for more details on the calculations underlying this estimate). Requiring annual penetration testing would increase industry costs for penetration testing by over 300 percent, to approximately $134,021,173 total and $19,081,600 annualized over a 10-year period of analysis, discounted at 7 percent. This alternative would result in an 18.7 percent increase in the total cost of the rule, bringing the total cost to industry and the

government to approximately $668,212,472 total and $95,138,423, annualized, over a 10-year period of analysis, discounted at 7 percent. The Coast Guard believes these increased costs are prohibitive and ultimately decided to reject this alternative. See table 52 for the costs associated with annual penetration testing over a 10-year period of analysis.

Using the estimated annualized cost of this alternative of approximately $95.1 million, and using the Maersk cyber-attack, we estimate the number of years this alternative would have to break even and to prevent at least one or more attacks of this type annually (with the same avoided losses) to be approximately 3.15 years ($300 million ÷ $95.1 million), compared with 3.75 years with the chosen alternative.

Table 52: Estimated Penetration Testing Costs of the Proposed Alternative for Facilities, OCS Facilities, and U.S.-Flagged Vessels (2022 Dollars, 10-year Discounted Costs, 7- and 3-percent Discount Rates)

Year	Facilities and OCS Facilities Cost	U.S.-Flagged Vessel Cost	Total Cost	7 Percent	3 Percent
1	$4,758,900	$14,322,700	$19,081,600	$17,833,271	$18,525,825
2	$4,758,900	$14,322,700	$19,081,600	$16,666,608	$17,986,238
3	$4,758,900	$14,322,700	$19,081,600	$15,576,270	$17,462,367
4	$4,758,900	$14,322,700	$19,081,600	$14,557,261	$16,953,754
5	$4,758,900	$14,322,700	$19,081,600	$13,604,917	$16,459,956
6	$4,758,900	$14,322,700	$19,081,600	$12,714,876	$15,980,540
7	$4,758,900	$14,322,700	$19,081,600	$11,883,061	$15,515,087
8	$4,758,900	$14,322,700	$19,081,600	$11,105,665	$15,063,191
9	$4,758,900	$14,322,700	$19,081,600	$10,379,126	$14,624,458
10	$4,758,900	$14,322,700	$19,081,600	$9,700,118	$14,198,502
Total	**$47,589,000**	**$143,227,000**	**$190,816,000**	**$134,021,173**	**$162,769,918**
Annualized				**$19,081,600**	**$19,081,600**

Note: Totals may not sum due to independent rounding.

(3) Penetration Testing at the Discretion of an Owner or Operator

Given the cost of penetration testing, particularly for small businesses with limited resources, the Coast Guard considered an alternative that would make penetration an optional provision. This would allow those in the affected population to choose to prioritize different cybersecurity measures. The decision to undertake penetration testing

could be made as a result of thorough risk assessments for each organization, considering its operational environments, risk profile, and pertinent threats.

Under this alternative, an owner or operator, or a CySO on their behalf, could determine when a penetration test is warranted, if at all. Because the testing would be optional, we assume that fewer owners and operators would conduct penetration testing in a given year, however, we have no way of knowing how many this would be. If none of the affected owners or operators elected to conduct penetration testing, this could hypothetically reduce costs for owners and operators for penetration testing down to zero, meaning a cost reduction of $28,549,669 and an annualized cost reduction of $4,064,831 over a 10-year period of analysis, discounted at 7 percent when compared to the preferred alternative.

However, the value of penetration testing for most organizations cannot be overstated. When integrated into a comprehensive cybersecurity strategy, penetration testing can be very effective in identifying vulnerabilities. By fostering a proactive rather than reactive approach in cybersecurity, penetration testing enables organizations to stay ahead of potential threats and better understand how malicious actors could exploit weaknesses in IT and OT systems. This is particularly crucial given the quickly evolving landscape of cyber threats. In addition, because the costs of a potential cyber incident could be high, with potential downstream economic impacts, the Coast Guard must prioritize some level of oversight on provisions that could lessen the risk of a cyber incident. Therefore, we rejected this alternative, despite the potential cost savings. It should be noted, however, that according to proposed § 101.665, owners and operators of facilities, OCS facilities, and U.S.-flagged vessels can seek a waiver or an equivalence determination if they are unable to meet the proposed requirements, penetration testing included.

With this alternative, the estimated annualized cost decreases to approximately $76.1 million compared with the chosen alternative. Using the Maersk cyber-attack, we estimate the number of years for this alternative to breakeven and to prevent at least one or more attacks of this type annually (with the same avoided losses) to be approximately 3.9 years ($300 million ÷ $76.1 million), compared with 3.75 years with the chosen alternative.

(4) Penetration Testing in Conjunction with Cybersecurity Plan Submission (Preferred Alternative)

In an effort to best balance the cost of annual penetration testing with the risk of leaving the MTS vulnerable to cyber incidents with even more costly impacts, the Coast Guard considered requiring penetration tests every 5 years, aligned with the renewal of a Cybersecurity Plan. This is the preferred alternative because penetration testing would supplement other cybersecurity measures in the proposed regulations such as vulnerability scanning, annual Cybersecurity Assessments and audits, quarterly drills, and annual exercises, which may limit the necessity of annual penetration testing. However, making penetration testing an optional requirement for organizations could inadvertently leave them more exposed to cyber-attacks and limit the Coast Guard's understanding of the MTS' cybersecurity readiness. Under the preferred alternative, owners and operators are still free to conduct more frequent tests at their discretion if they would like to increase their awareness of vulnerabilities. Alternatively, they could apply for waivers or exemptions if they feel like they cannot meet the proposed requirements related to penetration testing. Please see the "Breakeven Analysis" section of this RIA for the breakeven estimates of this chosen alternative.

B. Small Entities

Under the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, the Coast Guard has prepared this Initial Regulatory Flexibility Analysis (IRFA) that examines the impacts of this proposed rule on small entities.

Per the RFA, a small entity may be a small independent business, defined as one independently owned and operated, organized for profit, and not dominant in its field under the Small Business Act (5 U.S.C. 632); a small not-for-profit organization, defined as any not-for-profit enterprise which is independently owned and operated and is not dominant in its field; or a small governmental jurisdiction, defined as a locality with fewer than 50,000 people.

Section 603(b) of the RFA prescribes the content of the IRFA, which addresses the following:

(1) A description of the reasons why action by the agency is being considered;

(2) A succinct statement of the objectives of, and legal basis for, the proposed rule;

(3) A description of and, where feasible, an estimate of the number of small entities to which this proposed rule will apply;

(4) A description of the projected reporting, recordkeeping, and other compliance requirements to comply with the proposed rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record;

(5) An identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap, or conflict with this proposed rule; and

(6) A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the proposed rule on small entities.

1. Description of the reasons why action by the agency is being considered.

This proposed rule helps address current and emerging cybersecurity threats to maritime security in the MTS. Cybersecurity risks result from vulnerabilities in the operation of vital systems, which increase the likelihood of cyber-attacks on facilities, OCS facilities, and vessels. Cyber-related risks to the maritime domain are threats to the critical infrastructure that citizens and companies depend on to fulfill their daily needs.

Cyber-attacks on public infrastructure have raised awareness of the need to protect systems and equipment that facilitate operations within the MTS because cyber-attacks have the potential to disable the IT and OT of vessels, facilities, and OCS facilities. Autonomous vessel technology, automated OT, and remotely accessible machines provide additional opportunities for cyber-attackers. These systems and equipment are prime targets for cyber-attacks that could potentially disrupt vessel movements and shut down port operations, such as loading and unloading cargoes. Section III.A., *The Problem We Seek to Address*, and Section IV.A, *The Current State of Cybersecurity in the MTS* in this NPRM provide more details.

2. A succinct statement of the objective of, and legal basis for, the proposed rule.

The objective of this proposed rule is to establish minimum performance-based cybersecurity requirements for U.S.-flagged vessels, facilities, and OCS facilities subject to MTSA. The proposed requirements include account security measures, device security measures, data security measures, governance and training, risk management, supply chain management, resilience, network segmentation, reporting, and physical security.

The Coast Guard has statutory authority to promulgate regulations under 43 U.S.C. 1333(d); 46 U.S.C. 3306, 3703, 70102 through 70104, 70124; and DHS Delegation No. 00170, Revision No. 01.3. Section 4 of the Outer Continental Shelf Lands Act of 1953, codified as amended at 43 U.S.C. 1333(d), authorizes the Secretary to promulgate regulations with respect to safety equipment and other matters relating to the promotion of safety of life and property on the artificial islands, installations, and other

devices on the OCS. This authority was delegated to the Coast Guard by DHS Delegation No. 00170(II)(90), Revision No. 01.3.

Sections 70102 through 70104 in Title 46 of the U.S.C. authorize the Secretary to evaluate for compliance vessel and facility vulnerability assessments, security plans, and response plans. Section 70124 authorizes the Secretary to promulgate regulations to implement Chapter 701, including sections 70102 through 70104, dealing with vulnerability assessments for the security of vessels, facilities, and OCS facilities; VSPs, FSPs, and OCS FSPs; and response plans for vessels, facilities, and OCS facilities. These authorities were delegated to the Coast Guard by DHS Delegation No. 00170(II)(97)(a) through (c), Revision No. 01.3.

Section III.C. of this preamble, *Legal Authority to Address This Problem*, provides more details on the Coast Guard's legal basis for these actions.

3. A description of and, where feasible, an estimate of the number of small entities to which the proposed rule will apply.

This section considers the number of small entities likely to be affected by this NPRM. First, we determine which owners of facilities, OCS facilities, and vessels in the affected population qualify as small businesses, small not-for-profit organizations, or small governments. Then, we compare reported annual revenues among the identified small entities with annual compliance costs estimated by the Coast Guard.

Number of Small Entities Affected

To identify the portion of the affected facility, OCS facility, and vessel owners that are likely to be small businesses and small not-for-profit organizations, we match business-and organization-specific information with size standards for small businesses published in the Small Business Administration's (SBA) Table of Small Business Size

Standards.[127,128] The SBA defines small businesses in terms of firm revenues or number of employees. Size thresholds of small businesses differ depending on the industry sector, defined in terms of NAICS codes; therefore, the analysis also requires us to identify the relevant NAICS codes for the affected facility and vessel owners. To accomplish this, we take the following steps:

(1) Identify the names and addresses of owners of facilities, OCS facilities, and U.S.-flagged vessels using information contained in the Coast Guard's MISLE database;[129]

(2) Upload the names and location information to D&B Hoovers' website and rely on D&B Hoovers' proprietary algorithm to match entities with the information stored in its database;[130]

(3) Collect the primary NAICS code, ownership type,[131] number of employees,[132] and annual revenue information from entities that matched the information in D&B Hoovers' database; and

---

[127] SBA. "Table of size standards." Available at: https://www.sba.gov/document/support-table-size-standards. Effective March 17, 2023, accessed July 21, 2023.

[128] To determine whether not-for-profit organizations are small entities, we rely on the self-identified NAICS code reported by each organization to D&B Hoovers and the SBA's small business size standard for that NAICS code. Any organization qualifying as a small business pursuant to SBA's threshold is considered to be "not dominant in its field" (15 U.S.C. 632) and is categorized as a small organization. If no NAICS code is available, we assume the organization is small.

[129] The Coast Guard provided MISLE data to Industrial Economics, Incorporated (IEc) on June 2, 2023, and June 9, 2023.

[130] This process relies on D&B Hoovers' automated search functions to identify the business profiles associated with a list of businesses, not manual business-by-business searching. This search functionality is described in more detail in D&B Hoovers (2019, page 25). You can find this resource at https://app.dnbhoovers.com/product/wp-content/uploads/2020/10/DB-Hoovers-User-Guide-920.pdf. The matched data were downloaded from D&B Hoovers on June 20, 2023, accessed via: app.dnbhoovers.com/login, July 21, 2023.

[131] D&B Hoovers provides ownership type for the matched entities. This analysis considers all entities marked as "private," "public," or "partnership" as businesses. "Nonprofit" ownership status is used to identify not-for-profit organizations.

[132] D&B Hoovers contains data fields for both "employees at single site" and "employees at all sites." When both numbers are provided, we default to using the "employees at all sites" entry to capture the size of the larger parent company. When only the "employees at single site" information is available, we use that entry instead.

(4) Determine which owners are small businesses or small not-for-profit organizations based on the SBA's definitions of small businesses matched to each NAICS code.[133]

The RIA considers facilities, OCS facilities, and vessels owned by governments or quasi-government organizations separately.[134] Small governmental jurisdictions are defined as governments of cities, counties, towns, townships, villages, school districts, or special districts, with a population of less than 50,000 (5 U.S.C. 601). After using D&B Hoovers to identify a sample of Government owners, the 2020 U.S. Census informed our classification of Government jurisdictions.[135]

Facility and OCS Facility Owners

MISLE identifies 3,411 regulated facilities and OCS facilities. Of the facilities, 2,663 are associated with 1,334 unique owners, and 748 lack owner information.[136] Like the cost analysis, this analysis assumes the 748 facilities lacking owner information in MISLE are associated with an additional 374 unique owners, under the assumption that the average facility owner is associated with 2 regulated facilities. In total, this analysis assumes a total of 1,708 affected owners and operators of facilities and OCS facilities.

The names and location information of all 1,334 identifiable affected owners were uploaded to D&B Hoovers, and the search function returned information for 786 entities (59 percent) with at least one identified NAICS code. The 548 unmatched entities either do not have business profiles in D&B Hoovers or the owner's name and location

---

[133] In some cases, SBA provides a size standard for the NAICS code as well as an "exception" for a sub-set of businesses with specific activity types. This analysis does not consider the "exceptions" when classifying businesses and not-for-profit organizations as small.

[134] Government owners are identified using the "public sector" ownership status in D&B Hoovers. In most cases, the entities that fall into the "public sector" ownership type also have 92 NAICS codes.

[135] 2020 U.S. Census data accessed from: https://www.census.gov/quickfacts/, accessed July 21, 2023.

[136] Owners of facilities and OCS facilities are determined using various data files in MISLE. Owner information is not reported in a standard format for facilities and OCS facilities; therefore, considerable data cleaning was necessary to identify unique owner names and location information. This analysis assumes the sample of facilities with owner information identified is broadly representative of all regulated facilities. Additionally, D&B Hoovers further consolidated the list of affected owners of facilities and OCS facilities by identifying unifying parent companies for some owners thought to be independent businesses or organizations based on MISLE data.

information stored in MISLE does not match the business records on the website. Included among the owners that matched with records in D&B Hoovers were 770 businesses (98 percent of the matched owners), 11 not-for-profit organizations (1 percent), and 5 Governments (1 percent). The 770 businesses categorize into 186 NAICS codes.

Table 53 reports the number of businesses in the top 10 most frequently occurring NAICS codes, as well as the portion that meet the definition of small business. An additional row summarizes the businesses across the remaining 176 NAICS codes. As presented, 615 of 770 businesses (80 percent) qualify as small based on their revenue or number of employees. Additionally, the 11 not-for-profit organizations include 10 small organizations (91 percent). The 5 Government jurisdictions include no small Governments (0 percent). Under the assumptions that (1) the 374 owners of facilities and OCS facilities without owner information in MISLE are small entities and (2) all 548 of facilities and OCS facilities for which D&B Hoovers profiles are not available are small entities, we estimate 1,533 total small entities are affected by the requirements for facilities and OCS facilities in this proposed rule (90 percent of affected facility owners) (374 owners without identifying information in MISLE + 548 unmatched facility owners + 601 matched small businesses + 10 matched small organizations + 0 matched small Governments= 1,533 total small entities). See table 53.

Table 53: Number of Small Entities Affected by the Proposed Rule's Cybersecurity Requirements for Facilities and OCS Facilities

NAICS Code	Type of Industry	Size Standard Type	Size Standard Used	Total Affected Owners	Number of Affected Owners Classified as Small	Percent Small
488320	Marine Cargo Handling	Revenue	$47 million	57	39	68%
424720	Petroleum and Petroleum Products Merchant Wholesalers (except Bulk Stations and Terminals)	Employees	200	37	33	89%
221118	Other Electric Power Generation	Employees	650	22	21	95%
324110	Petroleum Refineries	Employees	1,500	22	21	95%
493190	Other Warehousing and Storage	Revenue	$36.5 million	22	9	41%
424710	Petroleum Bulk Stations and Terminals	Employees	225	19	19	100%
483212	Inland Water Passenger Transportation	Employees	550	18	18	100%
336611	Ship Building and Repairing	Employees	1,300	17	15	88%
488510	Freight Transportation Arrangement	Revenue	$20 million	17	11	65%
493110	General Warehousing and Storage	Revenue	$34 million	17	9	53%
176 Additional NAICS Codes	Various	Various	Various	522	420	80%
Matched Businesses	**Various**	**Various**	**Various**	**770**	**615**	**80%**
Matched Not-for-Profit Organizations	**Various**	**Various**	**Various**	**11**	**10**	**91%**
Matched Governments	**Public Sector**	**Population**	**50,000**	**5**	**0**	**0%**
Unmatched Facility Owners				**548**	**548**	**100%**
Owners Without Identifying Information in MISLE				**374**	**374**	**100%**
Total Affected Owners of Facilities and OCS Facilities				**1,708**	**1,547**	**91%**

Notes:

- The first 10 rows include the most frequently occurring NAICS codes among businesses in the sample of owners that matched in D&B Hoovers.
- NAICS codes and type of industry reflect the 2022 NAICS classification.
- Small businesses and small not-for-profit organizations were identified using the SBA's *Table of Small Business Size Standards* (March 17, 2023, version).
- The owners considered in this analysis were established from the Coast Guard's MISLE database and classified as small entities based on information obtained from D&B Hoovers and the 2020 U.S. Census.
- See the main text for further analytic details and assumptions.

Vessel Owners

Across the eight categories of vessels regulated by the Coast Guard and considered for this proposed rule, MISLE identifies over 10,000 vessels owned by 1,775 unique entities.[137] The names and location information of all 1,775 owners stored in MISLE were uploaded to D&B Hoovers, and the search function returned information for 1,006 entities (57 percent) with at least 1 NAICS code identified. Included among the entities that matched with records in D&B Hoovers were 989 businesses (98 percent of the matched owners), 11 not-for-profit organizations (1 percent), and 6 Government jurisdictions (1 percent). The 989 businesses categorize into 170 NAICS codes.

Table 53 reports the number of businesses in the top 10 most frequently occurring NAICS codes, as well as the portion that meet the definition of small business. An additional row summarizes the businesses across the remaining 160 NAICS codes.[138] As presented, 900 of 989 businesses (91 percent) qualify as small businesses based on their revenue or number of employees. Additionally, the 11 not-for-profit organizations include 9 small organizations (82 percent), and the 6 Government jurisdictions include 1 small Government (17 percent). Under the assumption that all 769 vessel owners for which D&B Hoovers profiles are not available are small entities, we estimate 1,633 total small entities are affected by the vessel requirements in this proposed rule (92 percent of affected vessel owners) (769 unmatched vessel owners + 854 matched small businesses + 9 matched small organizations + 1 matched small Government = 1,633 total small entities). See table 54.

---

[137] Like facilities and OCS facilities, unique businesses are determined using both organization name and address as stored in the Coast Guard's MISLE database. The information for owners is more complete for vessels than for facilities and OCS facilities in MISLE; all vessels include owner information. D&B Hoovers was able to identify unifying parent companies for some owners thought to be independent businesses or organizations based on MISLE data.

[138] Included in this group is NAICS code 99990 "unclassified." Because SBA does not propose a size standard for this code, we assume all entities with NAICS code 99990 are small. For the matched vessel owners, 46 entities are classified with this code in D&B Hoovers.

Table 54: Number of Small Entities Affected by the Proposed Cybersecurity Requirements for Vessels

NAICS Code	Type of Industry	Size Standard Type	Size Standard Used	Total Affected Owners	Number of Affected Owners Classified as Small	Percent Small
488330	Navigational Services to Shipping	Revenue	$47 million	118	108	92%
237990	Other Heavy and Civil Engineering Construction	Revenue	$45 million	87	72	83%
483211	Inland Water Freight Transportation	Employees	1,050	44	40	91%
487210	Scenic and Sightseeing Transportation, Water	Revenue	$14 million	33	28	85%
336611	Ship Building and Repairing	Employees	1,300	29	27	93%
483212	Inland Water Passenger Transportation	Employees	550	29	29	100%
488410	Motor Vehicle Towing	Revenue	$9 million	28	26	93%
441222	Boat Dealers	Revenue	$40 million	26	26	100%
488320	Marine Cargo Handling	Revenue	$47 million	24	23	96%
532490	Other Commercial and Industrial Machinery and Equipment Rental and Leasing	Revenue	$40 million	20	19	95%
160 Additional NAICS Codes	Various	Various	Various	551	456	83%
Matched Businesses	**Various**	**Various**	**Various**	**989**	**854**	**86%**
Matched Not-for-Profit Organizations	**Various**	**Various**	**Various**	**11**	**9**	**82%**
Matched Governments (all 92 NAICS codes)	**Public Sector**	**Population**	**50,000**	**6**	**1**	**17%**
Unmatched Vessel Owners				**769**	**769**	**100%**
Total Affected Vessel Owners				**1,775**	**1,633**	**92%**

Notes:

- The first 10 rows include the most frequently occurring NAICS codes among businesses in the sample of owners that matched in D&B Hoovers.
- NAICS codes and type of industry reflect the 2022 NAICS classification.
- Small businesses and small not-for-profit organizations were identified using the SBA's *Table of Small Business Size Standards* (March 17, 2023, version).
- The owners considered in this analysis were established from the Coast Guard's MISLE database and classified as small entities based on information obtained from D&B Hoovers and the 2020 U.S. Census.
- See the main text for further analytic details and assumptions.

Summary

Across the combined 3,483 affected owners of facilities, OCS facilities, or vessels, we estimate that 3,180 small entities (91 percent) may be affected, including small businesses, small not-for-profit organizations, and small Governments. Because this analysis assumes all owners for which NAICS codes, employment, or revenue information is unmatched in D&B Hoovers are small entities, the projected number of affected small entities may be overestimated.

Costs Relative to Revenues

This discussion compares the cost of the proposed changes per facility and vessel owner with annual revenues of affected small entities. Revenue information is obtained from D&B Hoovers for small businesses and small not-for-profit organizations. For small Governments, we use the *2021 State and Local Government Finance Historical Datasets and Tables* available through the U.S. Census.[139] We assume that the findings of this analysis are indicative of the impacts on entities for which revenue information is not readily available.

The RFA does not define a "significant effect" in quantitative terms. In its guidance to agencies on how to comply with the RFA, the SBA states, "[i]n the absence of statutory specificity, what is 'significant' will vary depending on the economics of the industry or sector to be regulated. The agency is in the best position to gauge the small entity impacts of its regulation."[140] One of the measures SBA uses to illustrate whether an impact could be significant, is to determine whether the cost per entity exceeds 1 percent of the gross revenues.[141] Therefore, this analysis considers the 1 percent threshold when analyzing these potential impacts.

---

[139] Data downloaded on July 14, 2023, from https://www.census.gov/data/datasets/2021/econ/local/public-use-datasets.html, accessed July 21, 2023.
[140] U.S. Small Business Administration (SBA). 2017. *A Guide for Government Agencies: How to Comply with the Regulatory Flexibility Act*. Available at https://advocacy.sba.gov/2017/08/31/a-guide-for-government-agencies-how-to-comply-with-the-regulatory-flexibility-act/, page 18, accessed July 21, 2023.
[141] Id. Page 19

Facility and OCS Facility Owners

Assuming that an owner or operator would need to implement each of the provisions required by this proposed rule, Coast Guard estimates that the highest single-year costs would be incurred in year 2 of the analysis period. We estimate the year 2 cost is $37,667 for an owner or operator with one facility or OCS facility. Each additional facility or OCS facility owned or operated would increase the estimated annual costs by the cost of an additional Cybersecurity Plan, since each facility or OCS facility will require an individual Cybersecurity Plan. For example, consider an entity that owns 4 facilities. The estimated cost to that entity in year 2 is calculated as follows: $37,667 + (3 × $8,414) = $62,909. Table 55 provides a breakdown of the costs per owner or operator of one facility or OCS facility. The text that follows provides more detail on these cost calculations.

Table 55: Summary of Total Costs of the Proposed Rule per Owner or Operator of One Facility and OCS Facility (2022 Dollars, 10-year Undiscounted Costs)

Year	Facility Count	Cybersecurity Plan	Drills and Exercises	Account Security Measures	Multifactor Authentication	Cybersecurity Training	Penetration Testing	Vulnerability Management	Cyber Incident Reporting	Total
1	1	$4,207	$841	$576	$20,100	$4,633	$0	$3,390	$13	$33,760
2	1	$8,414	$841	$576	$11,100	$4,633	$8,700	$3,390	$13	$37,667
3	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
4	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
5	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
6	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
7	1	$1,893	$841	$576	$11,100	$4,633	$8,700	$3,390	$13	$31,146
8	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
9	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
10	1	$4,207	$841	$576	$11,100	$4,633	$0	$3,390	$13	$24,760
Total										**$275,893**
Annualized										**$27,589**

Note: Totals may not sum due to independent rounding.

To estimate the cost for an individual owner or operator of a facility or OCS facility to develop, resubmit, conduct annual maintenance, and audit the Cybersecurity Plan, we use estimates provided earlier in the analysis. The hour-burden estimates are 100 hours to develop the Cybersecurity Plan (average hour burden), 10 hours to conduct annual maintenance of the Cybersecurity Plan (which would include amendments), 15 hours to renew Cybersecurity Plans every 5 years, and 40 hours to conduct annual audits of Cybersecurity Plans. Based on estimates from the Coast Guard's FSP and OCS FSP reviewers at local inspections offices, approximately 10 percent of Plans would need to be revised and resubmitted in the second year, which is consistent with the current resubmission rate for FSPs and OCS FSPs.

For renewals of Plans after 5 years (occurring in the seventh year of the analysis period), Plans would need to be further revised and resubmitted in approximately 10 percent of cases as well. However, in this portion of the analysis, we estimate costs as though the owner or operator will need to revise and resubmit their Plans in all cases resulting in a conservative (upper-bound) estimate of per-entity costs. We estimate the time for revision and resubmission to be about half the time to develop the Plan itself, or 50 hours in the second year of submission, and 7.5 hours after 5 years (in the seventh year of the analysis period). Because we include the annual Cybersecurity Assessment in the cost to develop Cybersecurity Plans, and we do not assume that owners and operators will wait until the second year of analysis to begin developing the Cybersecurity Plan or implementing related cybersecurity measures, we divide the estimated 100 hours to develop Plans equally across the first and second years of analysis. Using the CySO loaded hourly CySO wage of $84.14, we estimate the Cybersecurity Plan related costs by adding the total number of hours to develop, resubmit, maintain, and audit each year and multiplying by the CySO wage. For example, we estimate owners would incur $8,414 in costs in year 2 of the analysis period [1 facility × $84.14 CySO wage × (50 hours to

develop the Plan + 50 hours to revise and resubmit the Plan) = $8,414]. Table 56 displays the per-entity cost estimates for an owner or operator of one facility over a 10-year period of analysis. For an owner or operator with multiple facilities or OCS facilities, we estimate the total costs by multiplying the estimates in table 56 by the number of owned facilities.

Table 56: Cybersecurity Plan Related Costs per Owner or Operator of a Facility and OCS Facility (2022 Dollars, 10-year Undiscounted Costs)

Year	Facility Count	CySO Wage	Hours to Develop Plan	Hours to Resubmit Plan	Annual Maintenance Hours	Audit Hours	Total
1	1	$84.14	50	0	0	0	$4,207
2	1	$84.14	50	50	0	0	$8,414
3	1	$84.14	0	0	10	40	$4,207
4	1	$84.14	0	0	10	40	$4,207
5	1	$84.14	0	0	10	40	$4,207
6	1	$84.14	0	0	10	40	$4,207
7	1	$84.14	15	7.5	0	0	$1,893
8	1	$84.14	0	0	10	40	$4,207
9	1	$84.14	0	0	10	40	$4,207
10	1	$84.14	0	0	10	40	$4,207
Total							**$43,963**
Annualized							**$4,396**

Note: Totals may not sum due to independent rounding.

Similarly, we use earlier estimates for the calculation of per-entity costs for drills and exercises, implementing account security measures, implementing multifactor authentication, cybersecurity training, penetration testing, vulnerability management, and resilience.

For drills and exercises, we assume that a CySO on behalf of each owner and operator of a facility or OCS facility will develop cybersecurity components to add to existing physical security drills and exercises. This development is expected to take 0.5 hours for each of the 4 annual drills and 8 hours for an annual exercise. Using the loaded hourly wage for a CySO of $84.14, we estimate annual costs of approximately $841 per owner or operator of a facility or OCS facility [$84.14 CySO wage × ((0.5 hours × 4 drills) + (8 hours × 1 exercise)) = $841], as seen in table 55.

For account security measures, we assume that a database administrator on behalf of each owner or operator will spend 8 hours each year implementing and managing account security. Using the loaded hourly wage for a database administrator of $71.96, we estimate annual costs of approximately $576 ($71.96 database administrator wage × 8 hours = $576), as seen in table 55.

For multifactor authentication, we assume that an owner or operator of a facility or OCS facility will spend $9,000 in the initial year on average to implement a multifactor authentication system and spend approximately $150 per employee annually for system maintenance and support. Therefore, we estimate first year costs of approximately $20,100 [$9,000 implementation cost + ($150 support and maintenance costs × 74 average facility company employees)], and subsequent year costs of $11,100 ($150 support and maintenance costs × 74 average facility company employees), as seen in table 55.

For cybersecurity training, we assume that a CySO at a facility or OCS facility will take 2 hours each year to develop and manage cybersecurity training for employees, and employees at a facility or OCS facility will take 1 hour to complete the training each year. Using the estimated CySO wage of $84.14 and the estimated employee wages at a facility or OCS facility of $60.34, we estimate annual training costs of approximately $4,633 [($84.14 × 2 hours) + ($60.34 × 74 facility company employees × 1 hour)], as seen in table 55.

For penetration testing, we estimate costs only in the second and seventh years of analysis since tests are required to be performed in conjunction with submitting and renewing the Cybersecurity Plan. We assume that owners and operators of facilities or OCS facilities will spend approximately $5,000 per penetration test and an additional $50 per IP address at the organization to capture network complexity. We use the total number of company employees as a proxy for the number of IP addresses, since the Coast

Guard does not have data on IP addresses or the network complexity at a given company. As a result, we estimate second- and seventh-year costs of approximately $8,700 [$5,000 testing cost + ($50 × 74 employees)], as seen in table 55.

For vulnerability management, we assume that each facility or OCS facility will need to secure a vulnerability scanning program or software. Because vulnerability scans can occur in the background, we do not assume an additional hour burden associated with implementing or using a vulnerability scanner each year. Using the annual subscription cost of an industry leading vulnerability scanning software, we estimate annual costs of approximately $3,390, as seen in table 55.

Finally, for resilience, we assume that each owner or operator of a facility or OCS facility will need to make at least one cybersecurity incident report per year. While this is incongruent with historical data that shows the entire affected population of facilities and OCS facilities reports only 18 cybersecurity incidents per year, we are attempting to capture a complete estimate of what the costs of this proposed rule could be for an affected entity. As such, we estimate that a CySO will need to take 0.15 hours to report a cybersecurity incident to the NRC, leading to annual per entity costs of approximately $13 ($84.14 CySO wage × 0.15 hours), as seen in table 55.

As demonstrated in table 55, affected entities are expected to incur the highest costs in year 2 of this proposed rule. This analysis estimates the cost of this proposed rule in year 2 per affected small entity, using the information presented in table 55 and adjusting for the number of facilities and OCS facilities owned by the entity as recorded in MISLE. Among all 1,547 presumed small entities (see table 53), 833 owners (54 percent) are associated with one facility ($37,667 cost in year 2), and the average small entity owns approximately 2 facilities ($45,609 cost in year 2). The small entity with the highest projected cost owns 37 facilities ($340,571 cost in year 2).

Table 57 compares the estimated year 2 costs specific to each entity with the annual revenues of 416 small entities in our sample of affected facilities for which revenue information is provided in D&B Hoovers.[142] As shown, approximately 55 percent of small entities may incur costs that meet or exceed 1 percent of annual revenue in the second year of the rule [(61 + 168) ÷ 416 = 55 percent]. The small entity with the highest ratio cost-to-revenue ratio is projected to incur costs of 158 percent of its reported annual revenue.

Table 57: Revenue Impact of the Proposed Rule on Identified Small Entities Owning Facilities and OCS Facilities

% Revenue Impact	Greatest Annual Cost (Year 2)	
	Small Facility Owners with Known Revenue	Portion of Small Facilities with Known Revenue
<1%	187	45%
1-3%	61	15%
>3%	168	40%
Total	**416**	**100%**

Source: IEc calculations using data from the Coast Guard and D&B Hoovers. See text for details.
Notes:

- The 416 small entities included in this calculation represent the subset of small entities identified in table 52 for which sales data is provided in D&B Hoovers.
- This table includes only small businesses and small not-for-profit organizations because we did not identify any affected small governments in the matched sample. It is possible that some small governments are affected if they are included among the entities that did not match with an entity in the D&B Hoovers database.
- The compliance costs used in this analysis are calculated specific to the number of facilities owned by each affected small entity. The second year of implementing the provisions in this proposed rule is projected to have the highest costs and is therefore used in this analysis. See text for details.
- Totals may not sum due to rounding

Vessel Owners

The costs to owners and operators of U.S.-flagged vessels differ from the costs to owners and operators of facilities and OCS facilities and are more heavily influenced by the number of vessels owned. Table 58 presents the estimated fixed costs per entity regardless of the number of vessels owned and vessel type, equivalent to $10,877 per year on average across the first 10 years of implementing the provisions in this proposed

[142] Sales information is not available for 209 of the identified small businesses and small not-for-profit organizations with matched profiles in D&B Hoovers (33 percent of the 625 total matched small businesses and small not-for-profit organizations). This analysis does not identify small Governments among the set of owners with matched profiles in D&B Hoovers.

rule. The data and assumptions underlying these estimates are provided later in this section.

Table 58: Summary of Fixed Costs of the Proposed Rule per Owner or Operator of U.S.-flagged Vessels (2022 Dollars, 10-year Undiscounted Costs)

Year	Cybersecurity Plan	Drills and Exercises	Account Security Measures	Multifactor Authentication	Cybersecurity Training	Penetration Testing	Vulnerability Management	Cyber Incident Reporting	Total
1	$3,366	$841	$576	$9,000	$168	$0	$3,390	$13	$17,354
2	$6,731	$841	$576	$0	$168	$5,000	$3,390	$13	$16,719
3	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
4	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
5	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
6	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
7	$1,515	$841	$576	$0	$168	$5,000	$3,390	$13	$11,503
8	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
9	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
10	$4,039	$841	$576	$0	$168	$0	$3,390	$13	$9,027
Total									**$108,765**
Annualized									**$10,877**

Note: Totals may not sum due to independent rounding.

Several other categories of costs are dependent on the type and number of vessels owned by each entity. These costs are calibrated to the average number of employees by vessel type as well as a unique weighted hourly wage based on the personnel employed on the vessels.[143] Table 59 displays the average number of employees for each vessel type, including shoreside employees, and their unique weighted mean hourly wages. Table 60, which follows, displays the variable per-vessel costs associated with each type of vessel. To calculate the total estimated cost per entity in the population of U.S.-flagged vessels, we add the annual estimated costs per vessel and per vessel type from table 60 based on the number and types of vessels owned observed in MISLE to the fixed costs presented in table 58. For example, consider an entity that owns two passenger vessels subject to subchapter H. The estimated cost to that entity in year 2 is calculated as follows: (2 × $20,557) + $16,719 = $57,833.

Table 59: Summary of Employees and Wages by Vessel Type

Vessel Type	Number of Employees per Vessel (Includes Shoreside)	Weighted Mean Hourly Wage
MODU	372	$39.60
Subchapter I Vessels	82	$46.36
OSVs	16	$54.92
Subchapter H Passenger Vessels	85	$41.85
Subchapter K Passenger Vessels	35	$45.52
Subchapter M Towing Vessels	13	$51.28
Subchapter D and Combination Subchapters O&D Tank Vessels	40	$55.94
Subchapter D, O, or I Barges	0	$0.00
Subchapters K and T International Passenger Vessels	27	$44.59

Table 60: Summary of Annual Costs of the Proposed Rule per U.S.-flagged Vessels Based on Type of Vessel (2022 Dollars, Undiscounted Costs)

Vessel Type	Vessel Count	Multifactor Authentication	Cybersecurity Training	Penetration Testing (Years 2 and 7)[144]	Total
MODU	1	$55,800	$14,731	$18,600	$89,131
Subchapter I Vessels	1	$12,300	$3,802	$4,100	$20,202

[143] The average per-vessel employee counts were taken from manning requirements in the certificates of inspection in MISLE. We averaged the mariner counts listed for each vessel within a subpopulation of vessels, then applied a 1.33 shoreside employee modifier to account for non-mariner employees. The calculation of wage rates across vessel types are described in "Appendix A: Wages Across Vessel Types."
[144] When adding these costs to the fixed costs for owners and operators, only add the estimated penetration testing costs in years 2 and 7.

OSVs	1	$2,400	$879	$800	$4,079
Subchapter H Passenger Vessels	1	$12,750	$3,557	$4,250	$20,557
Subchapter K Passenger Vessels	1	$5,250	$1,593	$1,750	$8,593
Subchapter M Towing Vessels	1	$1,950	$667	$650	$3,267
Subchapter D and Combination Subchapters O&D Tank Vessels	1	$6,000	$2,238	$2,000	$10,238
Subchapter D, O, or I Barges	1	$0	$0	$0	$0
Subchapters K and T International Passenger Vessels	1	$4,050	$1,204	$1,350	$6,604

To estimate the cost for an owner or operator of a U.S.-flagged vessel to develop, resubmit, conduct annual maintenance, and audit the Cybersecurity Plan, we use estimates provided earlier in the analysis. The hour-burden estimates are 80 hours for developing the Cybersecurity Plan (average hour burden), 8 hours for conducting annual maintenance of the Cybersecurity Plan (which would include amendments), 12 hours to renew Cybersecurity Plans every 5 years, and 40 hours to conduct annual audits of Cybersecurity Plans. Based on estimates from Coast Guard VSP reviewers at MSC, approximately 10 percent of Plans would need to be resubmitted in the second year due to necessary revisions, which is consistent with the current resubmission rate for VSPs.

For renewing Cybersecurity Plans after 5 years (occurring in the seventh year of the analysis period), Plans would need to be further revised and resubmitted in approximately 10 percent of cases as well. However, in this portion of the analysis, we estimate costs as though the owner or operator will need to revise and resubmit their Plans in all cases resulting in a conservative (upper-bound) estimate of per-entity costs. We estimate the time for revision and resubmission to be about half the time to develop the Plan itself, or 40 hours in the second year of submission, and 6 hours after 5 years (in the seventh year of the analysis period).

Because we include the annual Cybersecurity Assessment in the cost to develop Cybersecurity Plans, and we do not assume that owners and operators will wait until the second year of analysis to begin developing the Cybersecurity Plan or implementing related cybersecurity measures, we divide the estimated 80 hours to develop plans equally across the first and second years of analysis. Using the loaded hourly CySO wage of $84.14, we estimate the Cybersecurity Plan-related costs by adding the total number of hours to develop, resubmit, maintain, and audit the Plan each year and multiplying that figure by the CySO wage. For example, we estimate owners and operators would incur approximately $6,731 in costs in year 2 of the analysis period [$84.14 CySO wage × (40 hours to develop the plan + 40 hours to revise and resubmit the Plan) = $6,731]. See table 61.

Table 61: Cybersecurity Plan Related Costs per Owner or Operator of a U.S.-flagged Vessel (2022 Dollars, 10-year Undiscounted Costs)

Year	CySO Wage	Hours to Develop Plan	Hours to Resubmit Plan	Annual Maintenance Hours	Audit Hours	Total
1	$84.14	40	0	0	0	$3,366
2	$84.14	40	40	0	0	$6,731
3	$84.14	0	0	8	40	$4,039
4	$84.14	0	0	8	40	$4,039
5	$84.14	0	0	8	40	$4,039
6	$84.14	0	0	8	40	$4,039
7	$84.14	12	6	0	0	$1,515
8	$84.14	0	0	8	40	$4,039
9	$84.14	0	0	8	40	$4,039
10	$84.14	0	0	8	40	$4,039
Total						**$39,885**
Annualized						**$3,989**

Note: Totals may not sum due to independent rounding.

For drills and exercises, we assume that a CySO on behalf of each owner and operator of a vessel will develop cybersecurity components to add to existing physical security drills and exercises. This development is expected to take 0.5 hours for each of the 4 annual drills and 8 hours for an annual exercise. Using the loaded hourly wage for a CySO of $84.14, we estimate annual costs of approximately $841 per vessel owner or

operator [$84.14 CySO wage × ((0.5 hours × 4 drills) + (8 hours × 1 exercise)) = $841], as seen in table 58.

For account security measures, we assume that a database administrator on behalf of each owner or operator of a vessel will spend 8 hours each year implementing and managing account security. Using the loaded hourly wage for a database administrator of $71.96, we estimate annual costs of approximately $576 ($71.96 database administrator wage × 8 hours = $576), as seen in table 58.

For multifactor authentication, we assume that a vessel owner or operator will spend $9,000 in the initial year on average to implement a multifactor authentication system and spend approximately $150 per employee annually for system maintenance and support. Therefore, we estimate first-year fixed costs of approximately $9,000 for all owners and operators, with annual costs in years 2 through 10 dependent on the number of employees for each type of vessel. For example, we estimate the first-year costs to an owner or operator of one OSV to be approximately $11,400 [$9,000 implementation cost + ($150 support and maintenance costs × 16 average employees per OSV)], and subsequent year costs of $2,400 ($150 support and maintenance costs × 16 average employees per OSV). Fixed per-entity implementation costs of $9,000 can be found in table 58 and variable per-vessel costs can be found in table 60.

For cybersecurity training, we assume that a CySO for each owner or operator of a vessel will take 2 hours each year to develop and manage employee cybersecurity training, and vessel employees will take 1 hour to complete the training each year. The per employee costs associated with training vary depending on the types and number of vessels and would be based on the average number of employees per vessel and the associated weighted hourly wage. For example, using the estimated CySO wage of $84.14 and the estimated OSV employee wage of $54.91, we estimate annual training costs of approximately $1,047 [($84.14 × 2 hours) + ($54.91 × 16 average employees per

OSV × 1 hour)]. Fixed per-entity costs of $168 can be found in table 58 and variable per-vessel costs can be found in table 60.

For penetration testing, we estimate costs only in the second and seventh years of analysis since tests are required to be performed in conjunction with submitting and renewing the Cybersecurity Plan. We assume that owners and operators of vessels will spend approximately $5,000 per penetration test and an additional $50 per IP address at the organization to capture network complexity. We use the average number of employees per vessel as a proxy for the number of IP addresses, since the Coast Guard does not have data on IP addresses or the network complexity at a given company. As a result, we estimate second- and seventh-year costs as follows: [$5,000 testing cost + ($50 × average number of employees per vessel)]. For example, we estimate second- and seventh-year cost of approximately $5,800 for an owner or operator of an OSV [$5,000 testing cost + ($50 × 16 average number of employees per OSV)]. Fixed per-entity costs of $5,000 can be found in table 58 and variable per-vessel costs can be found in table 60.

For vulnerability management, we assume that each owner or operator of a U.S.-flagged vessel will need to secure a vulnerability scanning program or software. Because vulnerability scans can occur in the background, we do not assume an additional hour burden associated with the implementation or use of a vulnerability scanner each year. Using the annual subscription cost of an industry leading vulnerability scanning software, we estimate annual costs of approximately $3,390, as seen in table 58.

Finally, for resilience, we assume that each owner or operator of a U.S.-flagged vessel will need to make at least one cybersecurity incident report per year. While this is incongruent with historical data that shows the entire affected population of vessels only reports two cybersecurity incidents per year on average, we are attempting to capture a complete estimate of what the costs of this proposed rule could be for an affected entity. As such, we estimate that a CySO will need to take 0.15 hours a year to report a

cybersecurity incident to the NRC, leading to annual per-entity costs of approximately $13 ($84.14 CySO wage × 0.15 hours), as seen in table 58.

This analysis calculates vessel owner-specific annual compliance costs based on the type and number of vessels associated with each small entity as identified in MISLE. For the small entities that own only barges, there are no variable costs per vessel, and we assume that they will only incur per-company costs related to the Cybersecurity Plan and developing drills and exercises, meaning the greatest per-owner costs would occur in year 2. Our analysis identifies 161 small entities that fall into this category and presumes this proposed rule will cost these entities $7,572 each in year 2 ($6,731 Cybersecurity Plan-related costs + $841 drills and exercises costs). For all other small entities that own vessels, the costs include a per-owner component as well as per-vessel costs that vary by vessel type, and the highest total annual costs per owner would also occur in year 2. Among the 1,472 small entities in this category, 770 owners (52 percent) are associated with 1 vessel (with an average cost of $23,271 in year 2). The average small entity owns 5 vessels (with an average cost of $32,850 in year 2), while the small entity with the highest projected costs owns 359 vessels (with a cost of $148,588 in year 2).[145]

Table 62 compares the entity-specific costs in year 2 with the greatest costs with the annual revenues of 793 small entities in our sample of affected facilities for which revenue information is provided in D&B Hoovers (for small businesses and small not-for-profit organizations) or the *2021 State and Local Government Finance Historical Datasets and Tables* available through the U.S. Census (for small Governments).[146] As shown, 59 percent of small entities may incur costs that meet or exceed 1 percent of annual revenue in the second year of the rule [(167 + 298) ÷ 793 = 59 percent]. The

[145] Values may not directly align with the incremental cost analysis due to rounding.
[146] Sales information is not available for 71 of the identified small businesses and small not-for-profit organizations with matched profiles in D&B Hoovers (8 percent of the 864 total matched small entities).

small entity with the highest cost-to-revenue ratio is projected to incur costs of 146 percent of its reported annual revenue.

Table 62: Revenue Impact of the Proposed Rule on Identified Small Entities Owning Vessels

% Revenue Impact	Greatest Annual Cost (Year 2)	
	Small Vessel Owners with Known Revenue	Portion of Small Vessel Owners with Known Revenue
<1%	328	41%
1-3%	167	21%
>3%	298	38%
Total	**793**	**100%**

Source: IEc calculations using data from the Coast Guard, D&B Hoovers, and *2021 State and Local Government Finance Historical Datasets and Tables* available through the U.S. Census. See text for details.
Notes:
- The 793 small entities included in this calculation represent the subset of small entities identified in Table 21 for which sales data is provided in D&B Hoovers or the *2021 State and Local Government Finance Historical Datasets and Tables*.
- The compliance costs used in this analysis are calculated specific to the number and type of vessels owned by each affected small entity. See text for details.
- Totals may not sum due to rounding

Summary

This IRFA characterizes the revenue impacts on small entities by projecting costs for each affected owner specific to the number and type of U.S.-flagged vessels as well as the number of facilities or OCS facilities owned according to data from the Coast Guard. There are two reasons the estimated compliance costs, and, therefore, the impacts on small entities, are likely to be overestimated. First, the approach we took to estimate costs assumes that all owners will incur costs associated with all provisions required in this proposed rule. However, it is highly likely that many affected owners already have invested in some of the cybersecurity measures before the publication of this proposed rule. Data available to the Coast Guard demonstrate this is the case for many facility and OCS facility owners, although whether those facility owners are small entities is uncertain.[147] Second, some affected owners are unlikely to have IT or OT systems to which this proposed rule will apply. Those owners will incur only the costs associated

[147] See footnote 69.

with requesting a waiver or equivalence, which are likely to be far less than the costs described in this section.

4. A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record

This proposed rule would call for a new collection of information under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501–3520. As defined in 5 CFR 1320.3(c), "collection of information" comprises reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. Section VI.D., *Collection of Information*, describes the title and description of the information collection, a description of those who must collect the information, and an estimate of the total annual burden. For a description of all other compliance requirements and their associated estimated costs, please see the preceding analysis of the per-entity costs of this proposed rule.

5. An identification, to the extent practicable, of all relevant Federal rules which may duplicate, overlap or conflict with the proposed rule

The Coast Guard has identified two primary areas of overlap with this proposed rule. First, under proposed § 101.645, the Coast Guard would require the CySO to maintain an effective means of communication to convey changes in cybersecurity conditions to the personnel of the U.S.-flagged vessel, facility, or OCS facility. The communication systems and procedures would need to allow for effective and continuous communications between security personnel at a vessel, facility, or OCS facility, vessels interfacing with a facility or an OCS facility, the cognizant COTP, and national and local authorities with security responsibilities. While these requirements would require the CySO to maintain means to specifically maintain communications regarding cybersecurity conditions, the Coast Guard believes there may be significant overlap with

communication requirements for physical security established in 33 CFR 105.235 for facilities, 106.240 for OCS facilities, and 104.245 for vessels. Accordingly, we do not estimate additional costs related to these communications systems, but we request public comment on this assumption and if this new cybersecurity-specific requirement would create additional burden.

Second, under proposed § 101.650(i), the Coast Guard would require affected owners or operators to limit physical access to OT and related IT equipment to only authorized personnel and confirm that all HMIs and other hardware are secured, monitored, and logged for personnel access, with access granted on a by-exception basis. While these requirements are specific to the physical security of IT and OT systems, there is some overlap with physical security requirements established in §§ 104.265 and 104.270 for vessels, §§ 105.255 and 105.260 for facilities, and §§ 106.260 and 106.265 for OCS facilities under which areas containing IT and OT systems should be designated restricted areas. Accordingly, we do not estimate additional costs related to these requirements but request public comment on this assumption and if these new cybersecurity-specific requirements would create additional burdens.

6. A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes and which minimize any significant economic impact of the rule on small entities

The purpose of this proposed rule is to safeguard the MTS against current and emerging threats associated with cybersecurity by adding minimum cybersecurity requirements to 33 CFR part 101. However, rather than making these requirements prescriptive, the Coast Guard is choosing to propose minimum performance-based cybersecurity requirements for the MTS. Like the existing requirements in 33 CFR parts 104, 105 and 106, the Coast Guard would allow owners and operators the flexibility to determine the best way to implement and comply with these new requirements. This

means that, while the Coast Guard may require the implementation of a multifactor authentication system, for example, it is up to the discretion of the impacted owner or operator to determine what shape or form that system may take, and how many resources should be expended to implement it. As a result, many of the cost estimates in this RIA and small entities analysis represent conservative (upper-bound) estimates as we attempt to capture costs for a wide range of affected owners and operators. Further, the Coast Guard proposes to make waivers and equivalencies available to affected owners and operators who feel they are unable to meet the requirements of this proposed rule, offering additional flexibility to small entities that are not able to meet the full requirements.

The Coast Guard also considered an alternative that would make the penetration testing requirements of this proposed rule optional for small entities. Given the nature of penetration testing, it can often come with a high cost, particularly for small entities with limited resources. Leaving the penetration testing requirements up to owner discretion could allow small entities in the affected population to prioritize different cybersecurity measures that may make more sense for their organization. The decision to undertake penetration testing could be made as a result of thorough risk assessments for each organization, considering its operational environments, risk profile, and pertinent threats. Under this alternative, an owner or operator, or a CySO on their behalf, could determine when a penetration test is warranted, if at all.

Because penetration testing would be optional, this could hypothetically reduce costs for owners and operators for penetration testing down to zero, meaning an estimated cost reduction of $8,700 in the second and seventh years of analysis for an owner or operator of facilities and OCS facilities. It would also lead to estimated cost reductions in the second and seventh years of $23,600 ($5,000 + $18,600) for owners and operators of MODUs, $9,100 ($5,000 + $4,100) for owners and operators of vessels under subchapter

I, $5,800 ($5,000 + $800) for owners and operators of OSVs, $9,250 ($5,000 + $4,250) for owners and operators of passenger vessels under subchapter H, $6,750 ($5,000 + $1,750) for owners and operators of passenger vessels under subchapter K, $5,650 ($5,000 + $650) for owners and operators of towing vessels under subchapter M, $7,000 ($5,000 + $2,000) for owners and operators of tank vessels under subchapter D and a combination of subchapters O&D, and $6,350 ($5,000 + $1,350) for owners and operators of international passenger vessels under subchapters K and T. The estimated cost reductions could be higher if ownership of multiple vessels is considered.

Despite the potential for minimizing economic impacts, however, the value of penetration testing for most organizations, including small entities, cannot be overstated. When integrated into a comprehensive cybersecurity strategy, penetration testing can be very effective in identifying vulnerabilities. By fostering a proactive rather than reactive approach in cybersecurity, penetration testing enables organizations to stay ahead of potential threats and better understand how malicious actors could exploit weaknesses in IT and OT systems. This is particularly crucial given the quickly evolving landscape of cyber threats. In addition, because the costs of a potential cyber incident are so high, the Coast Guard must prioritize some level of oversight on provisions that could lessen the risk of a cyber incident. Therefore, we rejected this alternative despite the potential cost reductions.

It should be noted, however, that according to proposed § 101.665, owners and operators of facilities, OCS facilities, and U.S.-flagged vessels can seek a waiver or an equivalence determination if they are unable to meet any proposed requirements, penetration testing included. The Coast Guard requests public comment on the alternative presented here, as well as any other alternatives or options related to the proposed provisions that would alleviate impacts on affected small entities.

Conclusion

The Coast Guard is interested in the potential impacts from this proposed rule on small entities (businesses and Governments), and we request public comment on these potential impacts. If you think that this proposed rule will have a significant economic impact on you, your business, or your organization, please submit a comment to the docket at the address under **ADDRESSES** in this proposed rule. In your comment, explain why, how, and to what degree you think this proposed rule would have an economic impact on you.

C. Assistance for Small Entities

Under section 213(a) of the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. 104-121, we want to assist small entities in understanding this proposed rule so that they can better evaluate its effects on them and participate in the rulemaking. If the proposed rule would affect your small business, organization, or governmental jurisdiction and you have questions concerning its provisions or options for compliance, please call or email the person in the **FOR FURTHER INFORMATION CONTACT** section of this proposed rule. The Coast Guard will not retaliate against small entities that question or complain about this proposed rule or any policy or action of the Coast Guard.

Small businesses may send comments on the actions of Federal employees who enforce, or otherwise determine compliance with, Federal regulations to the Small Business and Agriculture Regulatory Enforcement Ombudsman and the Regional Small Business Regulatory Fairness Boards. The Ombudsman evaluates these actions annually and rates each agency's responsiveness to small business. If you wish to comment on actions by employees of the Coast Guard, call 1-888-REG-FAIR (1-888-734-3247).

D. Collection of Information

This proposed rule would call for a new collection of information under the Paperwork Reduction Act of 1995, 44 U.S.C. 3501–3520. As defined in 5

CFR 1320.3(c), "collection of information" comprises reporting, recordkeeping, monitoring, posting, labeling, and other similar actions. The title and description of the information collection, a description of those who must collect the information, and an estimate of the total annual burden follow. The estimate covers the time for reviewing instructions, searching existing sources of data, gathering, and maintaining the data needed, and completing and reviewing the collection.

Title: Cybersecurity Plans.

OMB Control Number: 1625-new.

Summary of Collection of Information: This collection of information would be new. The Coast Guard would collect information from the owners and operators of vessels, facilities, and OCS facilities under 33 CFR part 101, subpart F. The information collection would be for the submission of Cybersecurity Plans, amendments to Cybersecurity Plans, and cyber incident reports proposed in 33 CFR 101.650.

Need for Information: The Coast Guard would be creating new cybersecurity requirements for vessel and facility owners and operators to mitigate or prevent a cyber incident from occurring. The information we would request from industry would be from (1) the development of Cybersecurity Plans, which would include details on implemented drills and exercise, training, and various cybersecurity measures in § 101.650 that might safeguard critical IT and OT systems from cyber incidents; (2) amendments to Cybersecurity Plans; and (3) reporting cyber incidents to the NRC.

Proposed Use of Information: The Coast Guard would use this information to determine if vessel and facility owners and operators have cybersecurity measures in place and to ensure that owners and operators are conducting periodic reviews of plans and testing their IT and OT systems for adequacy. Additionally, the Coast Guard would ensure vessel and facility owners and operators are reporting cyber incidents to the Coast Guard.

Description of the Respondents: The respondents are owners and operators of U.S.-flagged vessels, U.S. facilities, and OCS facilities.

Number of Respondents: The number of respondents would be about 1,775 U.S.-flagged vessel owners and operators and about 1,708 facility and OCS facility owners and operators. We assume that a CySO would be responsible for the reporting and recordkeeping requirements of the proposed rule on behalf of each owner and operator.

Frequency of Response: The number of responses to this proposed rule would vary annually.

Burden of Response: The burden of response would vary for each regulatory requirement.

Estimate of Total Annual Burden: The estimate of annual burden varies based on the year of analysis. For the initial year of analysis, the hour burden for Cybersecurity Plan activities and cyber incident reporting would be about 241,553 hours across the affected population. This is derived from the development of 3,411 facility and OCS facility Cybersecurity Plans for 50 hours each, 1,775 vessel Cybersecurity Plans for 40 hours each, and 20 cyber incidents being reported for 0.15 hours each [(3,411 × 50) + (1,775 × 40) + (20 × 0.15)].

For the second year of analysis, the hour burden for Cybersecurity Plan activities and cyber incident reporting would be about 265,723 hours across the affected population. The second year of analysis represents the highest estimated hour burden for all years of analysis. This is derived from the development of 3,411 facility and OCS facility Cybersecurity Plans for 50 hours each, 341 facility and OCS facility Cybersecurity Plans being revised and resubmitted for an additional 50 hours, 1,775 vessel Cybersecurity Plans for 40 hours each, 178 vessel Cybersecurity Plans being revised and resubmitted for an additional 40 hours, and 20 cyber incidents being reported

for 0.15 hours each [(3,411 × 50) + (341 × 50) + (1,775 × 40) + (178 × 40) + (20 × 0.15)].

For the third through the sixth years of analysis, and the eighth through the tenth years of analysis, when Cybersecurity Plans are being maintained and amendments are being developed, the hour burden for Cybersecurity Plan activities and cyber incident reporting would be about 48,313 hours across the affected population. This is derived from the maintenance and amendment of 3,411 facility and OCS facility Cybersecurity Plans for 10 hours each, the maintenance and amendment of 1,775 vessel Cybersecurity Plans for 8 hours each, and 20 cyber incidents being reported for 0.15 hours each [(3,411 × 10) + (1,775 × 8) + (20 × 0.15)].

For the seventh year of analysis, when Cybersecurity Plans are renewed, the hour burden for Cybersecurity Plan activities and cyber incident reporting would be about 76,094 hours across the affected population. This is derived from the renewal of 3,411 facility and OCS facility Cybersecurity Plans for 15 hours each, 341 facility and OCS facility Cybersecurity Plans being revised and resubmitted for an additional 7.5 hours, 1,775 vessel Cybersecurity Plans being renewed for 12 hours each, 178 vessel Cybersecurity Plans being revised and resubmitted for an additional 6 hours, and 20 cyber incidents being reported for 0.15 hours each [(3,411 × 15) + (341 × 7.5) + (1,775 × 12) + (178 × 6) + (20 × 0.15)].

This leads to an annualized hour burden total of 92,156 hours over the 10-year period of analysis.

As required by 44 U.S.C. 3507(d), we will submit a copy of this proposed rule to OMB for its review of the collection of information.

We ask for public comment on the proposed collection of information to help us determine, among other things—

- How useful the information is;

- Whether the information can help us perform our functions better;
- How we can improve the quality, usefulness, and clarity of the information;
- Whether the information is readily available elsewhere;
- How accurate our estimate is of the burden of collection;
- How valid our methods are for determining the burden of collection; and
- How we can minimize the burden of collection.

If you submit comments on the collection of information, submit them to both the OMB and to the docket indicated under **ADDRESSES**.

You need not respond to a collection of information unless it displays a currently valid control number from OMB. Before the Coast Guard could enforce the collection of information requirements in this proposed rule, OMB would need to approve the Coast Guard's request to collect this information.

E. Federalism

A rule has implications for federalism under Executive Order 13132 (Federalism) if it has a substantial direct effect on States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of Government. We have analyzed this proposed rule under Executive Order 13132 and have determined that it is consistent with the fundamental federalism principles and preemption requirements described in Executive Order 13132. Our analysis follows.

It is well settled that States may not regulate in categories reserved for regulation by the Coast Guard and that all categories covered in 46 U.S.C. 3306, 3703, 7101, and 8101 (design, construction, alteration, repair, maintenance, operation, equipping, personnel qualification, and manning of vessels), as well as the reporting of casualties and any other category in which Congress intended the Coast Guard to be the sole source of a vessel's obligations, are within the field foreclosed from regulation by the States.

See United States v. Locke, 529 U.S. 89 (2000). This proposed rule would expand maritime security requirements under MTSA to expressly address current and emerging cybersecurity risks and safeguard the MTS. In enacting MTSA, Congress articulated a need to address port security threats around the United States while preserving the free flow of interstate and foreign commerce. MTSA's mandatory, comprehensive maritime security regime, founded on this stated interest of facilitating interstate and international maritime commerce, indicates that States and local governments are generally foreclosed from regulating in this field. Particularly with respect to vessels subject to this new subpart F, the Coast Guard's above noted comprehensive law and regulations would preclude State and local laws. OCS facilities, which do not generally fall under any State or local jurisdiction, are principally subject to federal law and regulation.

Notwithstanding MTSA's general preemptive effect, States and local governments have traditionally shared certain regulatory jurisdiction with the Federal Government over waterfront facilities. Accordingly, current MTSA regulations make clear that the maritime facility security requirements of 33 CFR part 105 only preempt State or local regulation when the two conflict.[148] Similarly, the cybersecurity requirements of this proposed rule as they apply to a facility under 33 CFR part 105 would only have preemptive effect over a State or local law or regulation insofar as the two actually conflict (meaning compliance with both requirements is impossible or the State or local requirement frustrates an overriding Federal need for uniformity). In the unlikely event that state or local government would claim jurisdiction over an OCS facility, the aforenoted conflict preemption principles would apply.

In light of the foregoing analysis, this proposed rule is consistent with the fundamental federalism principles and preemption requirements described in Executive Order 13132.

---

[148] 33 CFR 101.112(b).

While it is well settled that States may not regulate in categories in which Congress intended the Coast Guard to be the sole source of a vessel's obligations, the Coast Guard recognizes the key role that State and local governments may have in making regulatory determinations. Additionally, for rules with federalism implications and preemptive effect, Executive Order 13132 specifically directs agencies to consult with State and local governments during the rulemaking process. If you believe this proposed rule would have implications for federalism under Executive Order 13132, please call or email the person listed in the **FOR FURTHER INFORMATION CONTACT** section of this preamble.

F. Unfunded Mandates

The Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1531–1538, requires Federal agencies to assess the effects of their discretionary regulatory actions. The Act addresses actions that may result in the expenditure by a State, local, or tribal government, in the aggregate, or by the private sector of $100 million (adjusted for inflation) or more in any one year.

Upon adjusting for inflation, this proposed action would need to result in the expenditure of $177 million or more in any one year, in 2022 dollars. To obtain this inflated value, we use the 2022 and 1995 annual gross domestic product implicit price deflator values of 127.224 and 71.823, respectively. We divide these values to obtain a factor of approximately 1.77, rounded (127.224 ÷ 71.823 = 1.77).[149] Multiplying this factor by the expenditure amount identified in the Unfunded Mandates Reform Act of 1995 gives us our expenditure amount adjusted for inflation (1.77 × 100,000,000 = 177,000,000). Because this proposed rule would result in the expenditure by the private

[149] We use the implicit price deflator for gross domestic product values from the Bureau of Economic Analysis National Income and Product Accounts interactive data tables. See https://apps.bea.gov/iTable/?reqid=19&step=3&isuri=1&1921=survey&1903=11#eyJhcHBpZCI6MTksInN0ZXBzIjpbMSwyLDMsM10sImRhdGEiOltbIk5JUEFfVGFibGVfTGlzdCIsIjEzIl0sWyJDYXRlZ29yaWVzIiwiU3VydmV5Il0sWyJGaXJzdF9ZZWFyIiwiMTk5NSJdLFsiTGFzdF9ZZWFyIiwiMjAyMyJdLFsiU2NhbGUiLCIwIl0sWyJTZXJpZXMiLCJBIl1dfQ==, accessed July 13, 2023.

sector of approximately $91,170,100 in undiscounted 2022 dollars in the most cost-heavy year, this proposed action would not require an assessment.

Although this proposed rule would not result in such an expenditure, we do discuss the potential effects of this proposed rule elsewhere in this preamble. Additionally, many of the provisions proposed in this NPRM are intentionally designed to take owner or operator discretion into account, which could help reduce anticipated expenditures. While this proposed rule may require action related to a security measure (implementing multifactor authentication, for example), the method or policy used to achieve compliance with the provision is at the discretion of the impacted owner or operator. This NPRM also includes the option for waivers and equivalents, in § 101.665, for any affected party unable to meet the requirements of this proposed rule. These intentional flexibilities can help reduce expected costs for those in the affected population and allow for more tailored cybersecurity solutions.

G. Taking of Private Property

This proposed rule would not cause a taking of private property or otherwise have taking implications under Executive Order 12630 (Governmental Actions and Interference with Constitutionally Protected Property Rights).

H. Civil Justice Reform

This proposed rule meets applicable standards in sections 3(a) and 3(b)(2) of Executive Order 12988, (Civil Justice Reform), to minimize litigation, eliminate ambiguity, and reduce burden.

I. Protection of Children

We have analyzed this proposed rule under Executive Order 13045 (Protection of Children from Environmental Health Risks and Safety Risks). This proposed rule is not an economically significant rule and would not create an environmental risk to health or risk to safety that might disproportionately affect children.

J. Indian Tribal Governments

This proposed rule does not have tribal implications under Executive Order 13175 (Consultation and Coordination with Indian Tribal Governments), because it would not have a substantial direct effect on one or more Indian tribes, on the relationship between the Federal Government and Indian tribes, or on the distribution of power and responsibilities between the Federal Government and Indian tribes.

K. Energy Effects

We have analyzed this proposed rule under Executive Order 13211 (Actions Concerning Regulations That Significantly Affect Energy Supply, Distribution, or Use). We have determined that it is not a "significant energy action" under that order because although it is a "significant regulatory action" under Executive Order 12866, it is not likely to have a significant adverse effect on the supply, distribution, or use of energy.

L. Technical Standards

The National Technology Transfer and Advancement Act, codified as a note to 15 U.S.C. 272, directs agencies to use voluntary consensus standards in their regulatory activities unless the agency provides Congress, through OMB, with an explanation of why using these standards would be inconsistent with applicable law or otherwise impractical. Voluntary consensus standards are technical standards (for example, specifications of materials, performance, design, or operation; test methods; sampling procedures; and related management systems practices) that are developed or adopted by voluntary consensus standards bodies.

This proposed rule does not use technical standards. Therefore, we did not consider the use of voluntary consensus standards.

M. Environment

We have analyzed this proposed rule under Department of Homeland Security Management Directive 023-01, Rev. 1, associated implementing instructions, and

Environmental Planning COMDTINST 5090.1 (series), which guide the Coast Guard in complying with the National Environmental Policy Act of 1969 (42 U.S.C. 4321−4370f), and have made a preliminary determination that this action is one of a category of actions that do not individually or cumulatively have a significant effect on the human environment. A preliminary Record of Environmental Consideration supporting this determination is available in the docket. For instructions on locating the docket, see the **ADDRESSES** section of this preamble.

This proposed rule would be categorically excluded under paragraphs A3 and L54 of Appendix A, Table 1 of DHS Instruction Manual 023–01–001–01, Rev. 1. Paragraph A3 pertains to promulgation of rules, issuance of rulings or interpretations, and the development and publication of policies, orders, directives, notices, procedures, manuals, advisory circulars, and other guidance documents, notably those of a strictly administrative or procedural nature; and those that interpret or amend an existing regulation without changing its environmental effect. Paragraph L54 pertains to regulations that are editorial or procedural. This proposed rule involves establishing minimum cybersecurity requirements in Coast Guard regulations such as account security measures, device security measures, governance and training, risk management, supply chain management, resilience, network segmentation, reporting, and physical security. This proposed rule would promote the Coast Guard's maritime security mission by establishing measures to safeguard the MTS against emerging threats associated with cybersecurity. This proposed rule also would promote the Coast Guard's marine environmental protection mission by preventing or mitigating marine environmental damage that could ensue due to a cybersecurity incident. We seek any comments or information that may lead to the discovery of a significant environmental impact from this proposed rule.

List of Subjects in 33 CFR Part 101

Harbors, Maritime security, Reporting and recordkeeping requirements, Security measures, Vessels, Waterways.

For the reasons discussed in the preamble, the Coast Guard is proposing to amend 33 CFR part 101 as follows:

PART 101 - MARITIME SECURITY: GENERAL

1. The authority citation for part 101 is revised to read as follows:

Authority: 46 U.S.C. 70101-70104 and 70124; 43 U.S.C. 1333(d); Executive Order 12656, 3 CFR 1988 Comp., p. 585; 33 CFR 1.05-1, 6.04-11, 6.14, 6.16, and 6.19; DHS Delegation No. 00170.1, Revision No. 01.3.

2. Amend part 101 by adding subpart F, consisting of §§ 101.600 through 101.670, to read as follows:

Subpart F—Cybersecurity

Sec.

§ 101.600 Purpose.

The purpose of this subpart is to set minimum cybersecurity requirements for vessels and facilities to safeguard and ensure the security and resilience of the Marine Transportation System (MTS).

§ 101.605 Applicability.

(a) This subpart applies to the owners and operators of U.S.-flagged vessels subject to 33 CFR part 104, U.S. facilities subject to 33 CFR part 105, and Outer Continental Shelf (OCS) facilities subject to 33 CFR part 106.

(b) This subpart does not apply to any foreign-flagged vessels subject to 33 CFR part 104.

§ 101.610 Federalism.

Consistent with § 101.112(b), with respect to a facility regulated under 33 CFR part 105 to which this subpart applies, the regulations in this subpart have preemptive effect over a State or local law or regulation insofar as the State or local law or regulation applicable to the facility conflicts with these regulations, either by actually conflicting or by frustrating an overriding Federal need for uniformity.

§ 101.615 Definitions.

Unless otherwise specified, as used in this subpart:

Approved list means an owner or operator's authoritative catalog for products that meet cybersecurity requirements.

Backup means a copy of physical or virtual files or databases in a secondary location for preservation. It may also refer to the process of creating a copy.

Credentials means a set of data attributes that uniquely identifies a system entity such as a person, an organization, a service, or a device, and attests to one's right to access to a particular system.

Critical Information Technology (IT) or Operational Technology (OT) systems means any Information Technology or Operational Technology system used by the vessel, facility, or OCS facility that, if compromised or exploited, could result in a transportation security incident, as determined by the Cybersecurity Officer (CySO) in the Cybersecurity Plan. Critical IT or OT systems include those business support services that, if compromised or exploited, could result in a transportation security

incident. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party.

Cyber incident means an occurrence that actually jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an Information System, or actually jeopardizes, without lawful authority, an Information System.

Cyber Incident Response Plan means a set of predetermined and documented procedures to respond to a cyber incident. It is a document that gives the owner or operator or a designated Cybersecurity Officer (CySO) instructions on how to respond to a cyber incident and pre-identifies key roles, responsibilities, and decision-makers. *Cyber threat* means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system. The term "cyber threat" does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cybersecurity Assessment means the appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes identification of relevant vulnerabilities and threats and determining the extent to which adverse circumstances or events could result in operational disruption and other harmful consequences.

Cybersecurity Officer, or CySO, means the person(s) designated as responsible for the development, implementation, and maintenance of the cybersecurity portions of the Vessel Security Plan (VSP), Facility Security Plan (FSP), or Outer Continental Shelf (OCS) FSP, and for liaison with the Captain of the Port (COTP) and Company, Vessel, and Facility Security Officers.

Cybersecurity Plan means a plan developed to ensure application and implementation of cybersecurity measures designed to protect the owners' or operators' systems and equipment, as required by this part. A Cybersecurity Plan is either included in a VSP, FSP, or OCS FSP, or is an annex to a VSP, FSP, or OCS FSP.

Cybersecurity risk means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism. It does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

Cybersecurity vulnerability means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

Encryption means any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

Executable code means any object code, machine code, or other code readable by a computer when loaded into its memory and used directly by such computer to execute instructions.

Exploitable channel means any information channel (such as a portable media device and other hardware) that allows for the violation of the security policy governing the information system and is usable or detectable by subjects external to the trusted user.

Firmware means computer programs (which are stored in and executed by computer hardware) and associated data (which is also stored in the hardware) that may be dynamically written or modified during execution.

Hardware means, collectively, the equipment that makes up physical parts of a computer, including its electronic circuitry, together with keyboards, readers, scanners, and printers.

Human-Machine Interface, or HMI, means the hardware or software through which an operator interacts with a controller for industrial systems. An HMI can range from a physical control panel with buttons and indicator lights to an industrial personal computer with a color graphics display running dedicated HMI software.

Information System means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software data, applications, communications, and people. It includes the application of Information Technology, Operational Technology, or a combination of both.

Information Technology, or IT, means any equipment or interconnected system or subsystem of equipment, used in the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Known Exploited Vulnerability, or KEV, means a computer vulnerability that has been exploited in the past.

Multifactor Authentication means a layered approach to securing data and applications where a system requires users to present a combination of two or more credentials to verify their identity for login.

Network means information system(s) implemented with a collection of interconnected components. A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. A network consists of two or more computers that are linked in order to share resources, exchange files, or allow electronic communications.

Network map means a visual representation of internal network topologies and components.

Network segmentation means a physical or virtual architectural approach that divides a network into multiple segments, each acting as its own subnetwork, to provide additional security and control that can help prevent or minimize the impact of a cyber incident.

Operational Technology, or OT, means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a change through the monitoring or control of devices, processes, and events.

Patching means updating software and operating systems to address cybersecurity vulnerabilities within a program or product.

Penetration test means a test of the security of a computer system or software application by attempting to compromise its security and the security of an underlying operating system and network component configurations.

Principle of least privilege means that an individual should be given only those privileges that are needed to complete a task. Further, the individual's function, not identity, should control the assignment of privileges.

Privileged user means a user who is authorized (and, therefore, trusted) to perform security functions that ordinary users are not authorized to perform.

Risk means a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (1) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

Software means a set of instructions, data, or programs used to operate a computer and execute specific tasks.

Supply chain means a system of organizations, people, activities, information, and resources for creating computer products and offering IT services to their customers.

Threat means any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system through unauthorized access, destruction, disclosure, modification of information, or denial of service.

Vulnerability means a characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Vulnerability scan means a technique used to identify hosts or host attributes and associated vulnerabilities.

§ 101.620 Owner or Operator.

(a) Each owner or operator of a vessel, facility, or OCS facility is responsible for compliance with the requirements of this subpart.

(b) For each vessel, facility, or OCS facility, the owner or operator must—

(1) Ensure a Cybersecurity Plan is developed, approved, and maintained;

(2) Define in Section 1 of the Cybersecurity Plan the cybersecurity organizational structure and identify each person exercising cybersecurity duties and responsibilities within that structure, with the support needed to fulfill those obligations;

(3) Designate, in writing, by name and by title, a CySO who is accessible to the Coast Guard 24 hours a day, 7 days a week, and identify how the CySO can be contacted at any time;

(4) Ensure that cybersecurity exercises, audits, and inspections, as well as the Cybersecurity Assessment, are conducted as required by this part and in accordance with the Cybersecurity Plan (see § 101.625(d)(1), (3), (6) and (7));

(5) Ensure that the vessel, facility, or OCS facility operates in compliance with the approved Cybersecurity Plan;

(6) Ensure the development, approval, and execution of the Cyber Incident Response Plan; and

(7) Ensure all cyber incidents are reported to the National Response Center (NRC) at the telephone number listed in § 101.305 of this part.

§ 101.625 Cybersecurity Officer.

(a) *Other duties.* The Cybersecurity Officer (CySO) may perform other duties within the owner's or operator's organization (vessel or facility), provided the person is able to perform the duties and responsibilities required of the CySO by this part.

(b) *Serving as CySO for Multiple Vessels, Facilities or OCS Facilities.* The same person may serve as the CySO for more than one vessel, facility, or OCS facility. If a person serves as the CySO for more than one vessel, facility, or OCS facility, the name of each location for which that person is the CySO must be listed in the Cybersecurity Plan of each vessel, facility, or OCS facility for which that person is the CySO.

(c) *Assigning Duties Permitted*. The CySO may assign security duties to other vessel, facility, or OCS facility personnel; however, the CySO retains ultimate responsibility for these duties.

(d) *Responsibilities.* For each vessel, facility, or OCS facility for which they are designated, the CySO must—

(1) Ensure that the Cybersecurity Assessment is conducted as required by this part;

(2) Ensure the cybersecurity measures in the Cybersecurity Plan are developed, implemented, and operating as intended;

(3) Ensure that an annual audit of the Cybersecurity Plan and its implementation is conducted and, if necessary, ensure that the Cybersecurity Plan is updated;

(4) Ensure the Cyber Incident Response Plan is executed and exercised;

(5) Ensure the Cybersecurity Plan is exercised in accordance with § 101.635(c) of this part;

(6) Arrange for cybersecurity inspections in conjunction with vessel, facility and OCS facility inspections;

(7) Ensure the prompt correction of problems identified by exercises, audits, or inspections;

(8) Ensure the cybersecurity awareness and vigilance of personnel through briefings, drills, exercises, and training;

(9) Ensure adequate cybersecurity training of personnel;

(10) Ensure all breaches of security, suspicious activity that may result in TSIs, TSIs, and cyber incidents are recorded and reported to the owner or operator;

(11) Ensure that records required by this part are maintained in accordance with § 101.640 of this part;

(12) Ensure any reports as required by this part have been prepared and submitted;

(13) Ensure that the Cybersecurity Plan, as well as proposed substantive changes (or major amendments) to cybersecurity measures included therein, are submitted for approval to the cognizant COTP or the Officer in Charge, Marine Inspections (OCMI) for facilities or OCS facilities, or to the Marine Safety Center (MSC) for vessels, prior to amending the Cybersecurity Plan, in accordance with § 101.630 of this part;

(14) Ensure relevant security and management personnel are briefed regarding changes in cybersecurity conditions on board the vessel, facility, or OCS facility; and

(15) Ensure identification and mitigation of all KEVs in critical IT or OT systems, without delay.

(e) *Qualifications*. The CySO must have general knowledge, through training or equivalent job experience, in the following:

(1) General vessel, facility, or OCS facility operations and conditions;

(2) General cybersecurity guidance and best practices;

(3) The vessel, facility, or OCS facility's Cyber Incident Response Plan;

(4) The vessel, facility, or OCS facility's Cybersecurity Plan;

(5) Cybersecurity equipment and systems;

(6) Methods of conducting cybersecurity audits, inspections, control, and monitoring techniques;

(7) Relevant laws and regulations pertaining to cybersecurity;

(8) Instruction techniques for cybersecurity training and education;

(9) Handling of Sensitive Security Information and security related communications;

(10) Current cybersecurity threat patterns and KEVs;

(11) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security; and

(12) Conducting and assessing cybersecurity drills and exercises.

§ 101.630 Cybersecurity Plan.

(a) *General*. The CySO must develop, implement, and verify a Cybersecurity Plan for each vessel, facility, or OCS facility. The Cybersecurity Plan must reflect all cybersecurity measures required in this subpart, as appropriate, to mitigate risks identified during the Cybersecurity Assessment. The Plan must describe in detail how the requirements of subpart F will be met. The Cybersecurity Plan may be included in a VSP or an FSP, or as an annex to the VSP or FSP.

(b) *Protecting Sensitive Security Information*. The Cybersecurity Plan is Sensitive Security Information and must be protected in accordance with 49 CFR part 1520.

(c) *Format*. The owner or operator must ensure that the Cybersecurity Plan consists of the individual sections listed in this paragraph. If the Cybersecurity Plan does not follow the order as it appears on the list, the owner or operator must ensure that the Plan contains an index identifying the location of each of the following sections:

(1) Cybersecurity organization and identity of the CySO;

(2) Personnel training;

(3) Drills and exercises;

(4) Records and documentation;

(5) Communications;

(6) Cybersecurity systems and equipment, with associated maintenance;

(7) Cybersecurity measures for access control, including the computer, IT, and OT access areas;

(8) Physical security controls for IT and OT systems;

(9) Cybersecurity measures for monitoring;

(10) Audits and amendments to the Cybersecurity Plan;

(11) Reports of all cybersecurity audits and inspections, to include documentation of resolution or mitigation of all identified vulnerabilities;

(12) Documentation of all identified, unresolved vulnerabilities, to include those that are intentionally unresolved due to owner or operator risk acceptance;

(13) Cyber incident reporting procedures in accordance with part 101 of this subchapter; and

(14) Cybersecurity Assessment.

(d) *Submission and approval*. Each owner or operator must submit one copy of their Cybersecurity Plan for review and approval to the cognizant COTP or the OCMI for the facility or OCS facility, or to the MSC for the vessel. A letter certifying that the Plan meets the requirements of this subpart must accompany the submission.

(1) The COTP, OCMI, or MSC will evaluate each submission for compliance with this part, and either—

(i) Approve the Cybersecurity Plan and return a letter to the owner or operator indicating approval and any conditional approval;

(ii) Require additional information or revisions to the Cybersecurity Plan and return a copy to the owner or operator with a brief description of the required revisions or additional information; or

(iii) Disapprove the Cybersecurity Plan and return a copy, without delay, to the owner or operator with a brief statement of the reasons for disapproval.

(iv) If the cognizant COTP, OCMI, or MSC requires additional time to review the plan, they have the authority to return a written acknowledgement to the owner or operator stating that the Coast Guard will review the Cybersecurity Plan submitted for approval, and that the U.S.-flagged vessel, facility, or OCS facility may continue to operate as long as it remains in compliance with the submitted Cybersecurity Plan.

(2) Owners or operators submitting one Cybersecurity Plan to cover two or more vessels or facilities of similar operations must ensure the Plan addresses the specific cybersecurity risks for each vessel or facility.

(3) A Plan that is approved by the COTP, OCMI, or MSC is valid for 5 years from the date of its approval.

(e) *Amendments to the Cybersecurity Plan*.

(1) Amendments to a Coast Guard-approved Cybersecurity Plan must be initiated by either—

(i) The owner or operator or the CySO; or

(ii) When the COTP, OCMI, or MSC finds that the Cybersecurity Plan no longer meets the requirements in this part, the Plan will be returned to the owner or operator with a letter explaining why the Plan no longer meets the requirements and requires

amendment. The owner or operator will have at least 60 days to amend the Plan and cure deficiencies outlined in the letter. Until the amendments are approved, the owner or operator must ensure temporary cybersecurity measures are implemented to the satisfaction of the Coast Guard.

(2) Major amendments, as determined by the owner or operator based on types of changes to their security measures and operational risks, to the Cybersecurity Plan must be proposed to the Coast Guard prior to implementation. Proposed amendments to the Cybersecurity Plan must be sent to the Coast Guard at least 30 days before the proposed amendment's effective date. The Coast Guard will approve or disapprove the proposed amendment in accordance with this part. An owner or operator must notify the Coast Guard by the most rapid means practicable as to the nature of the amendments , the circumstances that prompted these amendments, and the period these amendments are expected to be in place.

(3) If the owner or operator has changed, the CySO must amend the Cybersecurity Plan, without delay, to include the name and contact information of the new owner or operator and submit the affected portion of the Plan for review and approval in accordance with this part.

(4) If the CySO has changed, the Coast Guard must be notified without delay and the affected portion of the Cybersecurity Plan must be amended and submitted to the Coast Guard for review and approval in accordance with this part without delay.

(f) *Audits*. (1) The CySO must ensure that an audit of the Cybersecurity Plan and its implementation is performed annually, beginning no later than 1 year from the initial date of approval. The CySO must attach a report to the Plan certifying that the Plan meets the applicable requirements of this subpart.

(2) In addition to the annual audit, the CySO must audit the Cybersecurity Plan if there is a change in the owner or operator of the vessel, facility, or OCS facility, or if

there have been modifications to the cybersecurity measures, including, but not limited to, physical access, incident response procedures, security measures, or operations.

(3) Auditing the Cybersecurity Plan as a result of modifications to the vessel, facility, or OCS facility, or because of changes to the cybersecurity measures, may be limited to those sections of the Plan affected by the modifications.

(4) Personnel conducting internal audits of the cybersecurity measures specified in the Plan or evaluating its implementation must—

(i) Have knowledge of methods of conducting audits and inspections, as well as access control and monitoring techniques;

(ii) Not have regularly assigned cybersecurity duties for the vessel, facility, or OCS facility being audited; and

(iii) Be independent of any cybersecurity measures being audited.

(5) If the results of an audit require amending the Cybersecurity Plan, the CySO must submit, in accordance with this part, the amendments to the Coast Guard for review and approval no later than 30 days after completion of the audit with a letter certifying that the amended Plan meets applicable requirements of subpart F.

§ 101.635 Drills and Exercises.

(a) *General.* (1) Drills and exercises must be used to test the proficiency of the vessel, facility, and OCS facility personnel in assigned cybersecurity duties and the effective implementation of the VSP, FSP, OCS FSP, and Cybersecurity Plan. The drills and exercises must enable the CySO to identify any related cybersecurity deficiencies that need to be addressed.

(2) The drill or exercise requirements specified in this section may be satisfied with the implementation of cybersecurity measures required by the VSP, FSP, OCS FSP, and Cybersecurity Plan as the result of a cyber incident, as long as the vessel, facility, or

OCS facility achieves and documents attainment of drill and exercise goals for the cognizant COTP.

(b) *Drills.* (1) The CySO must ensure that at least one cybersecurity drill is conducted every 3 months. Cybersecurity drills may be held in conjunction with other security or non-security drills, where appropriate.

(2) Drills must test individual elements of the Cybersecurity Plan, including responses to cybersecurity threats and incidents. Cybersecurity drills must take into account the types of operations of the vessel, facility, or OCS facility; changes to the vessel, facility, or OCS facility personnel; the type of vessel a facility is serving; and other relevant circumstances.

(3) If a vessel is moored at a facility on a date a facility has planned to conduct any drills, the facility cannot require the vessel or vessel personnel to be a part of or participate in the facility's scheduled drill.

(c) *Exercises.* (1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be—

(i) Full-scale or live;

(ii) Tabletop simulation;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be vessel- or facility-specific, or part of a cooperative exercise program to exercise applicable vessel, facility, and OCS facility Cybersecurity Plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the cybersecurity program and must include the substantial and active participation of the CySO(s).

(6) If any corrective action identified during an exercise is needed, it must be addressed and documented as soon as possible.

§ 101.640 Records and Documentation.

All records, reports, and other documents mentioned in this subpart must be created and maintained in accordance with 33 CFR 104.235 for vessels, 105.225 for facilities, and 106.230 for OCS facilities. At a minimum, the records must be created for the following activities: training, drills, exercises, cybersecurity threats, incidents, and audits of the Cybersecurity Plan.

§ 101.645 Communications.

(a) The CySO must have a means to effectively notify owners or operators and personnel of a vessel, facility, or OCS facility of changes in cybersecurity conditions at the vessel, facility, and OCS facility.

(b) Communication systems and procedures must allow effective and continuous communications between vessel, facility, and OCS facility security personnel, vessels interfacing with a facility or an OCS facility, the cognizant COTP, and national and local authorities with security responsibilities.

§ 101.650 Cybersecurity Measures.

(a) *Account security measures*. Each owner or operator of a vessel, facility, or OCS facility must ensure, at a minimum, the following account security measures are in place and documented in Section 7 of the Cybersecurity Plan:

(1) Automatic account lockout after repeated failed login attempts must be enabled on all password-protected IT and OT systems.

(2) Default passwords must be changed before using any IT or OT systems.

(3) A minimum password strength must be maintained on all IT and OT systems that are technically capable of password protection.

(4) Multifactor authentication must be implemented on password-protected IT and remotely accessible OT systems.

(5) The principle of least privilege must be applied to administrator or otherwise privileged accounts on both IT and OT systems;

(6) The owner or operator must ensure that users maintain separate credentials on critical IT and OT systems; and

(7) The owner or operator must ensure that user credentials are removed or revoked when a user leaves the organization.

(b) *Device security measures*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following device security measures are in place and documented in Section 6 of the Cybersecurity Plan:

(1) Develop and maintain a list of approved hardware, firmware, and software that may be installed on IT or OT systems. Any hardware, firmware, and software installed on IT and OT systems must be on the owner- or operator-approved list.

(2) Ensure applications running executable code must be disabled by default on critical IT and OT systems. Exemptions must be justified and documented in the Cybersecurity Plan.

(3) Maintain an accurate inventory of network-connected systems, including designation of critical IT and OT systems; and

(4) Develop and maintain accurate documentation identifying the network map and OT device configuration information.

(c) *Data security measures*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following data security measures are in place and documented in Section 4 of the Cybersecurity Plan:

(1) Data logs must be securely captured, stored, and protected so that they are accessible only by privileged users; and

(2) All data, both in transit and at rest, must be encrypted using a suitably strong algorithm.

(d) *Cybersecurity training for personnel*. The training program to address requirements under this paragraph must be documented in Sections 2 and 4 of the Cybersecurity Plan.

(1) All personnel with access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must have cybersecurity training in the following topics:

(i) Relevant provisions of the Cybersecurity Plan;

(ii) Recognition and detection of cybersecurity threats and all types of cyber incidents;

(iii) Techniques used to circumvent cybersecurity measures;

(iv) Procedures for reporting a cyber incident to the CySO; and

(v) OT-specific cybersecurity training for all personnel whose duties include using OT.

(2) Key personnel with access to the IT or remotely accessible OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must also have cybersecurity training in the following additional topics:

(i) Understanding their roles and responsibilities during a cyber incident and response procedure; and

(ii) Maintaining current knowledge of changing cybersecurity threats and countermeasures.

(3) All personnel must complete the training specified in paragraphs (d)(1)(ii) through (v) of this section by [DATE 180 DAYS AFTER EFFECTIVE DATE OF THE

FINAL RULE], and annually thereafter. Key personnel must complete the training specified in paragraph (d)(2) of this section by [DATE 180 DAYS AFTER EFFECTIVE DATE OF THE FINAL RULE], and annually thereafter, or more frequently as needed. Training for new personnel not in place at the time of the effective date of this rule must be completed within 5 days of gaining system access, but no later than within 30 days of hiring, and annually thereafter. Training for personnel on new IT or OT systems not in place at the time of the effective date of this rule must be completed within 5 days of system access, and annually thereafter. All personnel must complete the training specified in paragraph (d)(1)(i) within 60 days of receiving approval of the Cybersecurity Plan. The training must be documented and maintained in the owner's or operator's records in accordance with 33 CFR 104.235 for vessels, 105.225 for facilities, and 106.230 for OCS facilities.

(e) *Risk management*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following measures for risk management are in place and documented in Sections 11 and 12 of the Cybersecurity Plan:

(1) *Cybersecurity Assessment.* Each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure completion of a Cybersecurity Assessment that addresses each covered vessel, facility, and OCS facility. A Cybersecurity Assessment must be conducted within 1 year from [EFFECTIVE DATE OF FINAL RULE] and annually thereafter. However, the Cybersecurity Assessment must be conducted sooner than annually if there is a change in ownership of a U.S.-flagged vessel, facility, or OCS facility; or if there are major amendments to the Cybersecurity Plan. In conducting the Cybersecurity Assessment, the owner or operator must—

(i) Analyze all networks to identify vulnerabilities to IT and OT systems and the risk posed by each digital asset;

(ii) Validate the Cybersecurity Plan;

(iii) Document recommendations and resolutions in the Facility Security Assessment (FSA)/Vessel Security Assessment (VSA), in accordance with 33 CFR 104.305, 105.305, and 106.305;

(iv) Document and mitigate any unresolved vulnerabilities; and

(v) Incorporate recommendations and resolutions from paragraph (e)(1)(iii) of this section into the Cybersecurity Plan through an amendment, in accordance with § 101.630(e) of this part.

(2) *Penetration Testing*. In conjunction with FSP, OCS FSP, or VSP renewal, the owner or operator or designated CySO must ensure that a penetration test has been completed. Following the penetration test, all identified vulnerabilities must be included in the FSA or VSA, in accordance with 33 CFR 104.305, 105.305, and 106.305.

(3) *Routine system maintenance.* Each owner or operator or a designated CySO of a vessel, facility, or OCS facility must ensure the following measures for routine system maintenance are in place and documented in Section 6 of the Cybersecurity Plan:

(i) Ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems, without delay;

(ii) Maintain a method to receive and act on publicly submitted vulnerabilities;

(iii) Maintain a method to share threat and vulnerability information with external stakeholders;

(iv) Ensure there are no exploitable channels directly exposed to internet-accessible systems;

(v) Ensure no OT is connected to the publicly accessible internet unless explicitly required for operation, and verify that, for any remotely accessible OT system, there is a documented justification; and

(vi) Conduct vulnerability scans as specified in the Cybersecurity Plan.

(f) *Supply chain*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following supply-chain measures are in place and documented in Section 4 of the Cybersecurity Plan:

(1) Consider cybersecurity capability as criteria for evaluation to procure IT and OT systems or services;

(2) Establish a process through which all IT and OT vendors or service providers notify the owner or operator or designated CySO of any cybersecurity vulnerabilities, incidents, or breaches, without delay; and

(3) Monitor and document all third-party remote connections to detect cyber incidents.

(g) *Resilience*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following measures for resilience are in place and documented in Sections 3 and 9 of the Cybersecurity Plan:

(1) Report any cyber incidents to the NRC, without delay, to the telephone number listed in § 101.305 of this part;

(2) In addition to other plans mentioned in this subpart, develop, implement, maintain, and exercise the Cyber Incident Response Plan;

(3) Periodically validate the effectiveness of the Cybersecurity Plan through annual tabletop exercises, annual reviews of incident response cases, or post-cyber incident review, as determined by the owner or operator; and

(4) Perform backup of critical IT and OT systems, with those backups being sufficiently protected and tested frequently.

(h) *Network segmentation*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following measures for network segmentation are in place and documented in Sections 7 and 8 of the Cybersecurity Plan:

(1) Implement segmentation between IT and OT networks; and

(2) Verify that all connections between IT and OT systems are logged and monitored for suspicious activity, breaches of security, TSIs, unauthorized access, and cyber incidents.

(i) *Physical security*. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following measures for physical security are in place and documented in Sections 7 and 8 of the Cybersecurity Plan:

(1) In addition to any other requirements in this part, limit physical access to OT and related IT equipment to only authorized personnel, and confirm that all HMIs and other hardware are secured, monitored, and logged for personnel access; and

(2) Ensure unauthorized media and hardware are not connected to IT and OT infrastructure, including blocking, disabling, or removing unused physical access ports, and establishing procedures for granting access on a by-exception basis.

§ 101.655 Cybersecurity Compliance Dates.

All Cybersecurity Plans mentioned in this subpart must be submitted to the Coast Guard for review and approval during the second annual audit following [EFFECTIVE DATE OF FINAL RULE], according to 33 CFR 104.415 for vessels, 33 CFR 105.415 for facilities, or 106.415 for OCS facilities.

§ 101.660 Cybersecurity Compliance Documentation.

Each owner or operator must ensure that the cybersecurity portion of their Plan and penetration test results are available to the Coast Guard upon request. The Alternative Security Program provisions are addressed in 33 CFR 104.140 for vessels, 105.140 for facilities, and 106.135 for OCS facilities.

§ 101.665 Noncompliance, Waivers, and Equivalents.

An owner or operator who is unable to meet the requirements in subpart F may seek a waiver or an equivalence determination using the provisions applicable to a vessel, facility, or OCS facility as outlined in 33 CFR 104.130, 104.135, 105.130, 105.135,

106.125, or 106.130. If an owner or operator is temporarily unable to meet the requirements in this part, they must notify the cognizant COTP or MSC, and may request temporary permission to continue to operate under the provisions as outlined in 33 CFR 104.125, 105.125, or 106.120.

§ 101.670 Severability.

Any provision of this subpart held to be invalid or unenforceable as applied to any person or circumstance shall be construed so as to continue to give the maximum effect to the provision permitted by law, including as applied to persons not similarly situated or to dissimilar circumstances, unless such holding is that the provision of this subpart is invalid and unenforceable in all circumstances, in which event the provision shall be severable from the remainder of this subpart and shall not affect the remainder thereof.

Linda Fagan,
Admiral, U.S. Coast Guard,
Commandant.

[FR Doc. 2024-03075 Filed: 2/21/2024 8:45 am; Publication Date: 2/22/2024]