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, DHS.

ACTION: Final rule; request for comments.

SUMMARY: The Coast Guard is updating its maritime security regulations by establishing minimum cybersecurity requirements for U.S.-flagged vessels, Outer Continental Shelf facilities, and facilities subject to the Maritime Transportation Security Act of 2002 regulations. This final rule addresses current and emerging cybersecurity threats in the marine transportation system by adding minimum cybersecurity requirements to help detect risks and respond to and recover from cybersecurity incidents. These include requirements to develop and maintain a Cybersecurity Plan, designate a Cybersecurity Officer, and take various measures to maintain cybersecurity within the marine transportation system. The Coast Guard is also seeking comments on a potential delay for the implementation periods for U.S.-flagged vessels.

DATES: This final rule is effective July 16, 2025.

Comment period for solicited comments: Comments on a potential 2-to-5-year delay for the implementation periods for U.S.-flagged vessels in Section VII of this preamble must be submitted by March 18, 2025.

ADDRESSES:

Docket: To view documents mentioned in this preamble as being available in the docket, go to *www.regulations.gov,* type USCG–2022–0802 in the search box, and click ''Search.'' Next, in the Document Type column, select ''Supporting & Related Material.''

Comment period for solicited additional comments: You may submit comments on the implementation periods for U.S.-flagged vessels discussed in Section VII of this preamble via the electronic Federal Docket Management System. 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 person in the **FOR FURTHER INFORMATION CONTACT** section of this final rule for alternate instructions.

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 Christopher Rabalais, Office of Design and Engineering Standards, 202–372–1375.

SUPPLEMENTARY INFORMATION:

Table of Contents for Preamble

I. Abbreviations

ABS American Bureau of Shipping
The Act James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Pub. L. 117–263)
AGCS Allianz Global Corporate and Specialty
AIS Automatic Identification System
AMSCs Area Maritime Security Committees
ANPRM Advance notice of proposed rulemaking
ASP Alternative Security Program
BLS Bureau of Labor Statistics
BSEE Bureau of Safety and Environmental Enforcement
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
CIRC Cyber Incident Reporting Council
CIRCIA Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA Cybersecurity and Infrastructure Security Agency
CISO Chief Information Security Officer
COTP Captain of the Port
CPG Cybersecurity Performance Goal
CRM Cyber risk management
CSF Cybersecurity Framework
CSO Company Security Officer
CSRC Computer Security Resource Center
CVC–WI Coast Guard's Office of Commercial Vessel Compliance's Work Instruction
CySO Cybersecurity Officer
DC3 Defense Cyber Crimes Center
DCISE Defense Industrial Base Collaborative Information Sharing Environment
DHS Department of Homeland Security
DOC Document of Compliance
DoD Department of Defense
FBI Federal Bureau of Investigation
FEMA Federal Emergency Management Agency
FR Federal Register
FRFA Final Regulatory Flexibility Analysis
FSA Facility Security Assessment
FSO Facility security officer
FSP Facility security plan
GPS Global Positioning System
HMI Human-machine interface
IACS International Association of Classification Societies
ICR Information collection request
IEc Industrial Economics, Incorporated
IMO International Maritime Organization
IP internet protocol
INMARSAT International Maritime Satellite
IRFA Initial Regulatory Flexibility Analysis
ISM International Safety Management
IT Information technology
KEV Known exploited vulnerability
LANTAREA Coast Guard Atlantic Area
MARSEC Maritime Security
MCAAG Maritime Cybersecurity Assessment and Annex Guide
MISLE Marine Information for Safety and Law Enforcement
MMC Merchant Mariner Credential
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
OCSLA Outer Continental Shelf Lands Act of 1953
OEWS Occupational Employment and Wage Statistics
OMB Office of Management and Budget

OSV Offshore supply vessel
OT Operational technology
PACS Physical Access Control Systems
PII Personally identifiable information
PRC People's Republic of China
PVA Passenger Vessel Association
QCEW Quarterly Census of Employment and Wages
RA Regulatory analysis
RO Recognized Organization
§ Section
SBA Small Business Administration
SME Subject matter expert
SMS Safety management system
SOLAS the International Convention for Safety of Life at Sea, 1974
TSA Transportation Security Administration
TSI Transportation security incident
UR Unified Requirement
U.S.C. United States Code
VHF Very high frequency
VSA Vessel Security Assessment
VSO Vessel Security Officer
VSP Vessel security plan

II. Executive Summary

The maritime industry faces increasing cybersecurity threats as it increasingly relies on cyber-connected systems. The purpose of this final rule is to safeguard the marine transportation system (MTS) against current and emerging threats associated with cybersecurity by adding minimum cybersecurity requirements to 33 CFR part 101 to help detect, respond to, and recover from cybersecurity risks that may cause transportation security incidents (TSIs). This final rule addresses risks from the increased interconnectivity and digitalization of the MTS and current and emerging cybersecurity threats to maritime security in the MTS with the additional minimum requirements specified below.

First, this final rule requires that owners or operators of U.S.-flagged vessels, facilities, or Outer Continental Shelf (OCS) facilities required to have a security plan under 33 CFR parts 104, 105, and 106 to develop and maintain a Cybersecurity Plan and Cyber Incident Response Plan. The Cybersecurity Plan must include seven account security measures for owners or operators of a U.S.-flagged vessel, facility, or OCS facility: (1) enabling of automatic account lockout after repeated failed log in attempts on all password protected information technology (IT) systems; (2) changing default passwords (or implementing other compensating security controls if unfeasible) before using any IT or operational technology (OT) systems; (3) maintaining a minimum password strength on all IT and OT systems technically capable of password protection; (4) implementing multifactor authentication on password-protected IT and remotely accessible OT systems; (5) applying the principle of least privilege to administrator or otherwise privileged accounts on both IT and OT systems; (6) maintaining separate user credentials on critical IT and OT systems; and (7) removing or revoking user credentials when a user leaves the organization.

The Cybersecurity Plan also must include four device security measure requirements: (1) develop and maintain a list of any hardware, firmware, and software approved by the owner or operator that may be installed on IT or OT systems; (2) ensure that applications running executable code are disabled by default on critical IT and OT systems; (3) maintain an accurate inventory of network-connected systems including those critical IT and OT systems; and (4) develop and document the network map and OT device configuration information. In addition, the Cybersecurity Plan must include two data security measure requirements: (1) ensure that logs are securely captured, stored, and protected and accessible only to privileged users, and (2) deploy effective encryption to maintain confidentiality of sensitive data and integrity of IT and OT traffic when technically feasible. Owners or operators of U.S.-flagged vessels, facilities, or OCS facilities must also prepare and document a Cyber Incident Response Plan that outlines instructions on how to respond to a cyber incident and identifies key roles, responsibilities, and decision-makers amongst personnel.

Owners or operators must also designate a Cybersecurity Officer (CySO) who must ensure that U.S.-flagged vessel, facility, or OCS facility personnel implement the Cybersecurity Plan and the Cyber Incident Response Plan. The CySO must also ensure that the Cybersecurity Plan is up to date and undergoes an annual audit. The CySO must also arrange for cybersecurity inspections, ensure that personnel have adequate cybersecurity training, record and report cybersecurity incidents to the owner or operator, and take steps to mitigate them.

With this final rule, the Coast Guard finalizes the requirements that were proposed in the notice of proposed rulemaking (NPRM), ''Cybersecurity in the Marine Transportation System,'' published on February 22, 2024.[1] We also respond to the public comments that we received to the NPRM and make several clarifications regarding the regulatory framework. The changes we make in this final rule as compared to the NPRM include the following:

Applicability

- Revised the language in § 101.605 to clarify that these cyber regulations apply to the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities required to have security plans under 33 CFR parts 104, 105, and 106.
- Added text to § 101.660 to clarify that Alternative Security Program (ASP) provisions apply to cybersecurity compliance documentation.

Definitions

- Revised the definition of ''backup'' in § 101.615 to remove the phrase ''in a secondary location'' and the implication that backups must be stored ''offsite.''
- Amended the definition of ''hazardous condition'' in § 160.202 by incorporating the term ''cyber incident.''
- Revised the definition of ''cybersecurity officer'' in § 101.615 to clarify that the owner or operator must designate a CySO, but that they also may designate an alternate CySO to assist in the duties and responsibilities at all times, including at times when the CySO may be away from the U.S.-flagged vessel, facility, or OCS facility.

Owner or Operator

- Amended § 101.620(b)(7) to clarify that all entities not subject to 33 CFR 6.16–1 must report all reportable cyber incidents to the National Response Center (NRC) and amended § 101.650(g)(1) to clarify that all entities not subject to 33 CFR 6.16–1 report reportable cyber incidents to the NRC without delay.

Cybersecurity Officer

- Removed the term ''major amendment'' from §§ 101.625(d)(13) (as well as 101.630(e)(2)) to prevent ambiguity about which amendments require resubmission of the Cybersecurity Plan and for consistency with existing requirements in 33 CFR parts 104, 105, and 106.
- Revised § 101.625(d)(10), regarding the CySO's responsibilities in reporting incidents, to refer to reportable cyber incidents, rather than breaches of security, suspicious activity that may result in TSIs. Breaches of security and suspicious activity reporting are already addressed under 33 CFR 101.305, whereas these regulations are meant to address the reporting of reportable cyber incidents as defined in this final rule.

Cybersecurity Plan

- Added references to OCS Facility Security Plans (FSPs) in § 101.630(a) to clarify that OCS FSPs follow the same

[1] 89 FR 13404.

requirements as Vessel Security Plans (VSPs) and FSPs.

- Revised § 101.630(d) to remove the requirement to submit a letter certifying that the Cybersecurity Plan meets the regulatory requirements.
- Revised § 101.630(e)(1)(ii) to clarify that the owner and operator will have at least 60 days to submit its proposed amendments, and to leave the timeframes for curing any deficiencies up to the local Captain of the Port (COTP) identifying them rather than requiring that entities cure any deficiencies within the 60-day period.
- Revised § 101.630(e)(2) to add new paragraph (e)(2)(i) to note that nothing in that section should be construed as limiting the owner or operator of a U.S.-flagged vessel, facility, or OCS facility from the timely implementation of such additional security measures as necessary to address exigent security situations.
- Revised § 101.655 to reflect that the Cybersecurity Plan must also be submitted to the Coast Guard for review and approval within 24 months of the effective date of this final rule, rather than during the second annual audit following the effective date.

Drills and Exercises

- Revised § 101.635(b)(1) to require two cybersecurity drills every 12 months instead of requiring at least one cybersecurity drill every 3 months and added ''as required by 33 CFR 104.230, 105.220, or 106.225,'' where appropriate.

Definitions

- Revised § 101.615 to add a definition for the term ''logs'' and revised § 101.650(c)(1) to refer to the term ''logs'' rather than ''data logs,'' consistent with guidance from the National Institute of Standards and Technology (NIST) and CISA's CPGs.
- Revised § 101.615 to change the definition of Cybersecurity Plan and the reference to Plan submission in § 101.630(a) to clarify that separate submissions are acceptable.
- Revised § 101.615 to change the definition of multifactor authentication from ''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'' to ''a layered approach to securing data and applications for a system that requires users to present more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are (1) something you know, (2) something you have, and (3) something you are.''

Cybersecurity Measures

- Revised § 101.650(a)(1) to remove the reference to OT systems and specified that the requirements in § 101.650(e)(1)(i) and (iv) are for critical IT and OT systems in accordance with the Cybersecurity Performance Goals (CPGs) of the Cybersecurity and Infrastructure Security Agency (CISA).
- Revised § 101.650(b) to clarify that each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the device security measures are in place, addressed in Section 6 of the Cybersecurity Plan, and made available to the Coast Guard upon request.
- Revised § 101.650(c)(2) to specify that effective encryption must be deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic and to require that only sensitive data be encrypted.
- Revised § 101.650(e)(1) to specify that owners and operators will need to conduct the cyber assessment within 24 months of the effective date of this final rule, which increases the timeframe from the originally required 12 months.
- Revised § 101.650(e)(1)(i) to limit the identification of vulnerabilities to only ''critical'' OT and IT systems rather than all OT and IT systems and revised § 101.650(e)(iv) to remove ''mitigate any unresolved vulnerabilities'' and, instead, require that the owner or operator ensure patching or implementation of documented compensating controls for all known exploited vulnerabilities (KEVs) in critical IT or OT systems, without delay.
- Revised § 101.650(e)(2) in this final rule to clarify that penetration testing must be completed in conjunction with renewing the Cybersecurity Plan and to specify that the CySO must submit a letter verifying that the test was conducted, as well as all vulnerabilities identified from the penetration testing.
- Revised § 101.650(f)(2) to remove the references to ''breaches'' and ''incidents'' and replaced them with ''reportable cyber incidents,'' consistent with the decision to define ''reportable cyber incident'' and use that term in these regulations. The definition of ''reportable cyber incident'' being an incident that leads to, or, if still under investigation, can reasonably lead to 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 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.
- Revised § 101.650(f)(2) to remove the references to ''breaches'' and ''incidents'' and replaced them with ''reportable cyber incidents,'' consistent with the decision to define ''reportable cyber incident'' and use that term in these regulations. The definition of ''reportable cyber incident'' being an incident that leads to, or, if still under investigation, can reasonably lead to 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 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.

Noncompliance, Waivers, and Equivalents

- Revised § 101.665 to clarify that an owner or operator, after completing the required Cybersecurity Assessment, may seek a waiver or an equivalence determination for the requirements in subpart F consistent with the waiver and equivalence provisions in 33 CFR parts 104, 105, and 106. A Cybersecurity Assessment is necessary so that an owner or operated can identify which requirements are unnecessary. These changes ensure consistency with other regulations for requesting waiver or equivalence.
- Revised § 101.665 to specify that owners or operators must notify the Coast Guard when they must temporarily deviate from the requirements rather than when they are temporarily unable to meet the requirements. This revised text is more consistent with other regulations regarding temporary waiver.

Compliance Dates

Table 1 shows the phased implementation schedule for this final rule. Note that the rule's effective date will be July 16, 2025. In Section VII of this preamble, we are requesting public comment on a potential 2-to-5-year delay for the implementation periods for U.S.-flagged vessels.

Table 1: Timing of This Final Rule's Requirements

Effective Dates	Provisions
Immediately Upon Effective Date of This Final Rule	Entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16-1 begin ensuring that all reportable cyber incidents are reported to the National Response Center (NRC). § 101.620(b)(7).
Within 6 Months From the Effective Date of this Final Rule and Annually Thereafter	All personnel must complete the training specified in § 101.650(d)(1)(ii) through (v) that includes recognition and detection of cybersecurity threats and all types of cyber incidents, techniques used to circumvent cybersecurity measures, procedures for reporting a cyber incident to the CySO, and OT-specific cybersecurity training (for all personnel whose duties include using OT). Key personnel must also complete the training specified in § 101.650(d)(2) about their roles and responsibilities during a cyber incident and response procedure and how to maintain current knowledge of changing cybersecurity threats and countermeasures. (Additional training requirements include the following: Training for new personnel not in place at the time of the effective date of this final 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 final rule must be completed within 5 days of system access, and annually thereafter.)
Within 24 Months from the Effective Date of This Final Rule	Owners and operators must designate, in writing, the CySO. § 101.620(b)(3) and (c)(1). Owners and operators must conduct the Cybersecurity Assessment within 24 months of the effective date of this final rule and annually thereafter (or sooner than annually if there is a change in ownership). § 101.650(e)(1). Owners and operators must submit the Cybersecurity Plan to the Coast Guard for approval within 24 months of the effective date of this final rule. § 101.655.
After Receiving Approval of the Cybersecurity Plan	Owners and operators must conduct cybersecurity drills at least twice each calendar year. Owners and operators must also conduct cybersecurity exercises at least once each calendar year with no more than 18 months between cybersecurity exercises. § 101.635(b)(1) and (c)(1). All personnel must complete the training specified in § 101.650(d)(1)(i) within 60 days of receiving approval of the Cybersecurity Plan. 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. § 101.660.

The Coast Guard estimates that this final rule creates costs for industry and Government of approximately $1.2 billion total and $138.7 million annualized, discounted at 2 percent (2022 dollars). This increased estimate

from the NPRM is primarily driven by increases to our estimates of costs related to cybersecurity drills, exercises, and penetration testing. Cost estimates are also increased due to updated affected population data. Benefits of this final rule include reduced risk and mitigation of cyber incidents to protect impacted entities and downstream economic participants, and improved protection of MTS business operations to build consumer trust and promote increased commerce in the U.S. economy. Additional benefits include improved minimum standards of cybersecurity to protect the MTS, which is vital to the U.S. economy and U.S. national security, and to avoid supply chain disruptions.

III. Basis and Purpose

A. Cybersecurity Threats

The purpose of this final rule is to safeguard the MTS against current and emerging threats associated with cybersecurity by adding minimum cybersecurity requirements to 33 CFR part 101 to help detect, respond to, and recover from cybersecurity risks that may cause TSIs. This final rule addresses current and emerging cybersecurity threats to maritime security in the MTS. The maritime industry is undergoing a significant transformation that involves the increased use of cyber-connected systems. While these increasingly interconnected and networked 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 a Russian-based cybercriminal group, DarkSide, conducted a ransomware attack that forced a major pipeline company to go offline, resulting in a weeklong shutdown of 5,500 miles of petroleum pipelines on the East Coast of the United States. Cybersecurity threats require the maritime community to effectively manage constantly changing risks to create a safe cyber environment.

This final rule creates a regulatory environment for cybersecurity in the maritime domain for U.S.-flagged vessels, facilities, and OCS facilities. Vulnerabilities in the operation of vital systems increase the risk of cyber-attacks. Unmitigated cyber-related risks to the maritime domain can compromise the critical infrastructure that people and companies depend on to fulfill their daily needs and that maintain the effective operation of the MTS.

A 2018 report by the Council of Economic Advisors (CEA) stated that ''[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.'' [2]

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 research on cybersecurity, protecting critical infrastructures, preparing future employees for the cybersecurity workforce, and enforcing the rule of law in cyberspace.'' [3]

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.'' [4] 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.'' [5]

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.'' [6] The CEA further stated that ''firms remain reluctant to increase their exposure to legal and public affairs risks. The lack of information on cyber-attacks 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.'' [7]

This final rule applies to the owners and operators of U.S.-flagged vessels required to have a security plan under 33 CFR part 104 (Maritime Security: Vessels), facilities required to have a security plan under 33 CFR part 105 (Maritime Security: Facilities), and OCS facilities required to have a security plan under 33 CFR part 106 (Marine Security: Outer Continental Shelf (OCS) Facilities).

B. Legislation, Regulations, and Policy

In the Maritime Transportation Security Act of 2002 (MTSA),[8] Congress provided a framework for the Secretary of Homeland Security (''Secretary''), acting through the Coast Guard,[9] 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 FSPs, OCS FSPs, and VSPs, to review and approve such plans, and to conduct inspections and take enforcement actions.[10] The Coast Guard's implementing regulations address a range of considerations to prevent TSIs to the maximum extent practicable [11] and require, among other general and specific measures, security assessments and measures related to radio and telecommunication systems, including computer systems and networks.[12]

The Coast Guard has also issued additional guidance and policies to help regulated entities address potential cyber incidents in FSPs, OCS FSPs, and VSPs,[13] including a cybersecurity risk

[2] Economic Report of the President Together with the Annual Report of the Council of Economic Advisers 323–24 February 2018, *https://www.govinfo.gov/content/pkg/ERP-2018/pdf/ERP-2018.pdf*, accessed August 12, 2024.

[3] Id. at 324–25.

[4] Id. at 326

[5] Id.

[6] Id.

[7] Id.

[8] Pub. L. 107–295, 116 Stat. 2064, November 25, 2002.

[9] 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. 01.4.

[10] *See generally, for example,* 46 U.S.C. 70103.

[11] *See* 46 U.S.C. 70103(c)(1).

[12] *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 (d)(2)(v).

[13] 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

Continued

assessment model that was issued in January 2023,[14] and voluntary guidance issued to Area Maritime Security Committees (AMSCs) in July 2023.[15] Congress has repeatedly reaffirmed the MTSA framework, including through amendments passed in 2016,[16] 2018,[17] and 2021.[18] In the 2018 amendments, Congress amended MTSA to specifically require VSPs, FSPs, and OCS FSPs to include provisions for detecting, responding to, and recovering from cybersecurity risks that may cause TSIs.[19] By doing so, Congress explicitly identified cybersecurity risk as an area of specific concern in the maritime domain that deserved focused governmental regulatory effort. These regulations fall squarely within the MTSA authorities that Congress expressly expanded to address cybersecurity risk. The 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 46 U.S.C. 70103). The amendments provide more detailed mandatory baseline requirements for U.S.-flagged vessels and facilities subject to MTSA.

In response to the growing national security threat from malicious cyber actions, presidential policy over the last three presidential administrations has advanced cybersecurity in the maritime domain. Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity) recognized the Federal Government's role to secure our nation's critical infrastructure by working with the private sector—including owners and operators of U.S.-flagged vessels, facilities, and OCS facilities—to prepare for, prevent, mitigate, and respond to cybersecurity threats.[20]

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.[21] The National Emergency with Respect to Significant Malicious Cyber-Enabled Activities was extended on March 26, 2024.[22]

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.'' [23]

On July 28, 2021, the President issued the ''National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,'' [24] which required the Secretary of Homeland Security to coordinate with the Secretary of Commerce (through the Director of NIST) and other agencies, as appropriate, to develop baseline CPGs. These baseline CPGs will 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.'' [25] The Coast Guard relied on CISA's CPGs as a benchmark for technical requirements in this final rule.

On February 21, 2024, the President signed Executive Order 14116 (Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States), amending 33 CFR part 6 regulations, which are issued pursuant to 46 U.S.C. 70051.[26] In that Order, the President found that ''the security of the United States is endangered by reasons of disturbance in the international relations of the United States that exist as a result of persistent and increasingly sophisticated malicious cyber campaigns against the United States, and that such disturbances continue to endanger such relations.''

The Executive Order expanded the regulatory authorities of the Coast Guard COTP, a designated officer of the Coast Guard, to address, inspect, and search vessels when there is an articulable cybersecurity threat; take possession and control of vessels within the territorial waters of the United States; and prevent access of things (including data, information, network, program, system, or other digital infrastructure) to vessels or waterfront facilities whenever it appears that such actions are necessary to prevent damage or injury, including damage to any data, information, network, program, system, or other digital infrastructure on such vessel, or to any vessel, waterfront facility, or the waters of the United States.[27] Furthermore, the Commandant's authority was extended to prescribe conditions and restrictions relating to waterfront facilities and vessels in port, specifically to ''prevent, detect, assess, and remediate an actual or threatened cyber incident.'' [28] The Commandant exercised this authority in a February 21, 2024 Maritime Security (MARSEC) Directive.[29]

The Executive Order also amended the reporting requirement in 33 CFR part 6 to add CISA and to also require the reporting of actual or threatened cyber incidents. The amended 33 CFR 6.16–1 now requires the reporting of ''evidence of sabotage, subversive activity, or an actual or threatened cyber incident[s] involving or endangering any vessel, harbor, port, or waterfront facility'' to the Federal Bureau of Investigation (FBI), CISA, and the COTP or their respective representatives.[30]

Commercial Vessel Compliance's (CG–CVC) Vessel CRM Work Instruction CVC–WI–027(3), *Vessel Cyber Risk Management Work Instruction,* October 11, 2023, *https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/CVC-WI-27(3)b.pdf,* accessed January 6, 2025.

[14] *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. 12, 2024. The MCAAG was developed in coordination with the National Maritime Security Advisory Committee (NMSAC), AMSCs, and other maritime stakeholders. The guide serves as a resource for baseline Cybersecurity Assessments and Plan development and helps stakeholders address vulnerabilities that can lead to transportation security incidents.

[15] NVIC 09–02, Change 6.

[16] Pub. L. 114–120, 130 Stat. 27, February 8, 2016.

[17] Pub. L. 115–254, 132 Stat. 3186, October 5, 2018.

[18] Pub. L. 116–283, 134 Stat 4754, January 1, 2021.

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

[20] 78 FR 11739, February 19, 2013.

[21] 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.

[22] 89 FR 21427, March 27, 2024.

[23] 86 FR 26633, May 17, 2021.

[24] 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/,* accessed on July 24, 2023.

[25] CISA, ''Cross-Sector Cybersecurity Performance Goals,'' *https://www.cisa.gov/cross-sector-cybersecurity-performance-goals*, accessed August 12, 2024.

[26] 89 FR 13971, February 26, 2024.

[27] 33 CFR 6.04–5, 6.04–7, and 6.04–8.

[28] 33 CFR 6.14–1.

[29] Issuance of Maritime Security (MARSEC) Directive 105–4: Cyber Risk Management for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies, 89 FR 13726, Feb. 23, 2024.

[30] 89 FR 13971, 13973, February 26, 2024.

OCS facilities are not required to report under Part 6.

In 2021, the Coast Guard published its Cyber Strategic Outlook (CGCSO) to highlight the importance of managing cybersecurity risks in the MTS.[31] 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.[32] As outlined in the CGCSO's second line of effort, ''Protect the MTS,'' the Coast Guard has implemented a risk-based regulatory, compliance, and assessment regime. We have established 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.[33] Specifically, this final rule promulgates the Coast Guard's baseline cybersecurity regulations for U.S.-flagged vessels and 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 (NMSAC), AMSCs, and other maritime stakeholders, consistent with the activities described in section 2(e) of the National Institute of Standards and Technology Act (specifically, 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 final rule expands and clarifies 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 definition in this final rule.

C. Legal Authority

The Coast Guard is promulgating 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. 00170.1, Revision No. 01.4.

Section 4 of the Outer Continental Shelf Lands Act of 1953 (OCSLA), classified 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 thereto. This authority was delegated to the Coast Guard by DHS Delegation No. 00170.1(II)(90), Revision No. 01.4.

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, 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. 00170.1(II)(92)(b), Revision No. 01.4.

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. 00170.1(II)(92)(b), Revision No. 01.4.

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, which must address cybersecurity risks. 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 and facilities (which include OCS facilities); security plans for vessels, facilities, and OCS facilities; and response plans for vessels, facilities, and OCS facilities. These authorities were delegated to the Coast Guard by DHS Delegation No. 00170.1(II)(97)(a) through (c), and (n), Revision No. 01.4.

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. These developments, to a large extent, rely on IT systems and OT systems, which also increases potential cyber vulnerabilities and risks. Cybersecurity risks result from vulnerabilities to vital systems that increase the likelihood of cyber-attacks on U.S.-flagged vessels, facilities, and OCS facilities.

Cyber-attacks on critical infrastructure across multiple sectors have raised awareness of the need to protect the systems and equipment that facilitate operations within the MTS because cyber-attacks have the potential to disable the IT and OT on board U.S.-flagged vessels, 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 can 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 can result in accidents at sea, potential environmental disasters like oil spills,

[31] U.S. Coast Guard, ''Cyber Strategic Outlook,'' August 2021, *https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf,* accessed August 13, 2024.

[32] 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 August 12, 2024.

[33] The Coast Guard is aware that some entities already follow industry standards related to cybersecurity. The minimum requirements seek to establish a common baseline for all the regulated vessels, facilities, and OCS facilities that is not incompatible with such standards, recognizing that in some instances these minimums may increase a requirement, but in other circumstances may already be satisfied. The owner or operator can indicate within their Cybersecurity Plan that they are following a particular standard and highlight how their compliance with that standard satisfies Coast Guard requirements.

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 final 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 will 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,*[34] and MSC Resolution 428(98).[35] 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 final rule establishes a baseline level of protection throughout the MTSA-regulated vessel fleet. Having regulatory oversight over U.S.-flagged vessels, the Coast Guard can ensure these cybersecurity regulations are implemented appropriately by approving Cybersecurity Plans and conducting routine inspections. As discussed in Section VII of this preamble, the Coast Guard requests public comment on a potential 2-to-5-year delay for the implementation periods for U.S.-flagged vessels. (See the **ADDRESSES** portion of this preamble, under *Comment period for solicited additional comments,* for instructions on submitting comments.) This final rule also applies to facilities regulated by 33 CFR part 105 and OCS facilities regulated by 33 CFR part 106.

B. Current MTSA 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 [36] (85 FR 16108, March 20, 2020), the Coast Guard interpreted 33 CFR parts 105 and 106 as requiring owners and operators of 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. The NVIC provides non-binding guidance on how regulated entities can address these issues.

This final rule also expands upon the agency's previous 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 allows owners and operators the flexibility to determine the best way to implement and comply with these new requirements. Following the effective date of this final rule, personnel must complete certain training requirements within approximately 6 months, and owners or operators must sequentially complete a Cybersecurity Assessment and submit the Cybersecurity Plan to the Coast Guard for review and approval within 24 months. The Cybersecurity Plan also includes designating the CySO. These implementation periods allow sufficient time for the owners and operators of applicable U.S.-flagged vessels, facilities, and OCS facilities to comply with the requirements of this final rule.[37]

V. Discussion of Comments and Changes

In response to the NPRM we published on February 22, 2024,[38] we received 99 written submissions to our docket. These written submissions are available in the public docket for this rulemaking, where indicated under the **ADDRESSES** portion of the preamble, or use the direct link *www.regulations.gov/docket/USCG-2022-0802.* The Coast Guard appreciates the comments from the public, as these insights continue to inform Coast Guard actions and programs. Below, we summarize the comments and our responses.

Extension of Comment Period and Public Meetings

The Coast Guard received a number of comments about extending the initial comment period of 60 days for additional time to review the proposed rule and the impacts. The requests asked for additional time ranging from 30 to 90 days, with 30 days being the most common request. After considering these comments, we extended the comment period by 30 days through May 22, 2024.[39] The Coast Guard determined that the extended comment period offered sufficient opportunity for industry stakeholders, and the general public to express their feedback on the NPRM.

One commenter requested that we hold a public hearing during which they could ask us questions and receive further information before submitting a public comment on the NPRM. The Coast Guard did not grant this request. Any public meeting that we held would include a presentation about the contents of the NPRM and an opportunity for members of the public to submit oral comments, but it is unlikely that we would have been able to share information materially different than the information that was already provided in the published NPRM.

One commenter requested that the Coast Guard hold a series of ''industry days'' focused on specific threats to the maritime stakeholders.

This comment was received on May 22, 2024, the day the extended comment period closed, which did not allow time to consider this request or hold a public meeting or series of ''industry days'' before the end of the comment period. Additionally, we had already extended the comment period to allow for more time for industry to submit comments about specific impacts to the maritime industry. We received many comments during that period and have carefully considered them in developing this final rule.

[34] *https://wwwcdn.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 August 13, 2024.

[35] 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 August 13, 2024.

[36] See footnote 13.

[37] Existing general requirements to address cyber issues in security plans will continue to apply during this rulemaking.

[38] 89 FR 13404.

[39] 89 FR 24751.

A. General Comments

Several commenters submitted positive comments. Commenters commended us for strengthening cybersecurity and noted that the rule is needed, is very important for the marine transportation system, and is a ''great idea.'' One commenter supported our inclusion of specific proposals regarding device security measures in § 101.650(b). Another commenter supported requirements for vulnerability scanning and penetration testing. One commenter noted that the increasing interconnectivity of ports expands the attack surface and vulnerabilities exploitable by cyber actors.

The Coast Guard agrees with the commenter. We are finalizing this regulation to help mitigate these risks.

Out of Scope Comments

We received several comments that were out of scope for this rulemaking. One commenter expressed concern about the ship-to-shore cranes manufactured in the People's Republic of China (PRC).

Specific language to address PRC-manufactured cranes is outside the scope of this regulation, which establishes general, baseline cybersecurity requirements for regulated entities.

Another commenter asked for a list of crane manufacturers or providers impacted by MARSEC Directive 105–4 related to the PRC-manufactured cranes.

The Coast Guard announced the availability of MARSEC Directive 105–4 on February 23, 2024, which provided actions for owners or operators of ship-to-shore cranes manufactured by the PRC to manage cybersecurity risks (89 FR 13726). This MARSEC Directive was announced at the same time as the NPRM for this final rule, but its requirements are separate. Interested parties should refer to the notice of availability for MARSEC Directive 105–4.[40]

One commenter noted that CPGs specific to the maritime subsector should be prioritized. The commenter also inquired about how feasible it was to incorporate risk-based assessment processes into the MST [Marine Science Technician] ''A'' School curriculum.

The Coast Guard is not currently working on sector-specific CPGs. Entities are welcome to use their preferred references and standards to help inform their required Assessments and Plans. ''A'' school curricula are outside the scope of this regulation.

[40] 89 FR 13726, February 23, 2024.

Formalizing Training

One commenter stated that the Coast Guard needs to consider continuously monitoring OT devices and asked the Coast Guard to formalize training, leverage industry best practices to apply to maritime operations, and implement a ''Bug Bounty'' program like that of the Department of Defense (DoD).[41]

The commenter did not give additional information or a reason why the Coast Guard should formalize the training. While formal training can be beneficial, the Coast Guard will not mandate a specific training format. It is up to the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to assess the necessary level of training based on their unique cyber threats and risks.

This final rule provides minimum baseline standards. Owners and operators are welcome to implement additional cybersecurity measures if they wish, including leveraging industry best practices, continuous monitoring of OT devices, and establishing processes for vulnerability notification such as the ''Bug Bounty'' program. However, these additional measures are not required by this final rule.

Identity Protection and Authentication

Another commenter applauded the inclusion of identity protection and authentication practices, and noted that some current practices, such as ''bring your own device'' and ''work from anywhere'' models, increase the risks of relying on traditional authentication methods and further weaken obsolescent legacy security technologies.

The Coast Guard agrees that the rule's provisions appropriately address current cybersecurity risks.

Automated Technologies

One commenter advised caution regarding ''unchecked reliance'' on automated technologies and processes in the maritime industry. The commenter also noted the lack of Federal regulations for ''smart'' containers. Another commenter recommended that the Coast Guard's cybersecurity regulations should require private stakeholders to collaborate with DHS to ensure national security and protect American dockworkers from cyber-attacks and risks from automated technologies.

These comments fall outside the scope of the regulations, as our intent is not to address specific issues associated with ''smart'' containers in particular. This final rule focuses on cybersecurity threats and risks that may impact OT and IT systems on board vessels and at facilities.

One commenter noted that some ports and ships are becoming ''smart'' with use of artificial intelligence, algorithms, and other IT solutions. The commenter argued that the proposed regulations fell short of addressing the cybersecurity risks of more sophisticated systems by only providing minimum baseline requirements.

These regulations provide minimum baseline requirements that allow each owner or operator to customize the Cybersecurity Plan to the needs of their organization. We expect that organizations with more sophisticated systems, such as those described by the commenter, will use the Cybersecurity Assessment to identify their specific cybersecurity needs, which will then be accounted for in the Plan. The structure of this final rule provides each owner or operator the flexibility to customize their Plan based on their own needs and also to add other requirements they deem appropriate for their organization.

Additional Inspections

One commenter recommended that any vessel that visits an ''adversarial controlled shipyard'' for maintenance or repair should necessitate thorough inspections following the maintenance.

This is outside the scope of this rulemaking. We did not propose any requirements for such inspections and do not have any plans to pursue them at this time.

Rulemaking Process

One commenter suggested that issuing an advance notice of proposed rulemaking (ANPRM) first would have improved the process for crafting these regulations.

The Coast Guard considered an ANPRM, but ultimately decided that it was not necessary for this rulemaking project. We received robust comments on the NPRM that provided useful input on the cybersecurity regulations we proposed and that we have carefully considered in developing this final rule.

Several commenters stated that the Coast Guard did not engage with industry stakeholders before the release of the NPRM.

While we did not engage with industry on the NPRM specifically prior to its release, the Coast Guard regularly engages with MTS industry and other stakeholders on cyber and other risks at Government agency- or industry-hosted conferences and workshops, and other forums. In these engagements, we

[41] A ''Bug Bounty'' program is an initiative that rewards individuals for reporting bugs and vulnerabilities in software.

discuss the Coast Guard's current cyber posture in terms of vessel and facility compliance with MTSA. Cybersecurity presents challenging problems, along with a need to address them promptly to implement critical cybersecurity measures.

Port Security Grant Program

Some commenters requested that the Port Security Grant Program account for, or even give prioritization to, smaller facilities to address cybersecurity concerns.

The Coast Guard will seek to work with the Federal Emergency Management Agency (FEMA) to further highlight cybersecurity through the FEMA-administered Port Security Grant Program. Because we do not manage that program, we cannot make any representation about future prioritization of grant funds. As noted in FEMA's Fiscal Year 2024 Notice of Funding Opportunity for this program, all entities subject to an Area Maritime Transportation Security Plan, as defined by 46 U.S.C. 70103(b), may apply for program funding.[42] Eligible applicants include but are not limited to port authorities, facility operators, and State, local, and territorial government agencies.[43] FEMA identified enhancing cybersecurity as a key priority for Fiscal Year 2024.[44]

Coast Guard Experience With Enforcing Cybersecurity

Some commenters stated that they did not feel that the Coast Guard had the expertise to enforce these regulations or to conduct cybersecurity inspections. They also stated that the nature of personnel rotations among active-duty military meant that members would constantly require training, and the Coast Guard could not retain the expertise necessary to review and approve the Cybersecurity Plans. Some also felt that reviews of the Cybersecurity Plan should be held in a centralized location, due to the COTP not having enough cybersecurity expertise.

The Coast Guard maintains a diverse workforce of military and civilian personnel to balance the need to maintain institutional knowledge while keeping the ability to flexibly assign personnel to a wide range of billets and locations. Whether it is knowledge of commercial vessel safety regulations, hazardous materials regulations, or these new cybersecurity regulations, the Coast Guard will ensure adequately trained personnel will be available to enforce these regulations, including through reviewing Cybersecurity Plans. Although this final rule addresses training requirements for regulated entities and not Coast Guard personnel, the Coast Guard will ensure appropriate, adequate training is available for the personnel conducting associated work and missions. Additionally, the Coast Guard recognizes the comment regarding centralized reviews of the Cybersecurity Plans. The Coast Guard has not yet identified where ownership of initial and subsequent review of Cybersecurity Plans will reside, but will determine that upon assessing the process that optimizes resources and expertise. Whatever the Coast Guard determines, it will not alter the requirements for developing and submitting such Plans.

In addition, the Coast Guard has significant experience with the maritime security of vessels, facilities, and OCS facilities. We have specific cybersecurity units and capabilities dedicated to identifying threats and risks and to protecting the cybersecurity of the United States. We work in partnership with the DoD and other DHS components, specifically CISA and the Transportation Security Administration (TSA). We are confident that, by leveraging this experience and these partnerships, along with additional training, we can enforce the requirements in this final rule.

Some commenters asked if the Coast Guard planned to allow Recognized Organizations (ROs) to assist with reviewing Cybersecurity Plans.

The Coast Guard currently does not plan to allow ROs to assist with reviewing Cybersecurity Plans, but regulated entities may consult with ROs to ensure compliance with this final rule if they choose.

B. Comments Related to the Applicability of This Final Rule

One commenter asked us to clearly define the scope of the Coast Guard's jurisdictional authority to regulate cybersecurity as it applies to marine infrastructure.

As discussed in the legal authority section, the Coast Guard has statutory authority under MTSA, as amended and codified at 46 U.S.C. chapter 701, to regulate cybersecurity in the MTS. As already long-established by the existing regulations in 33 CFR subchapter H, MTSA is applicable to the vessels, facilities, and OCS facilities that are subject to this final rule. The authority to regulate ''cybersecurity risk'' was specifically added to MTSA by the Maritime Security Improvement Act of 2018.[45]

One commenter explained that some ports oversee airports under their jurisdiction and thus, have dual cybersecurity requirements with the Federal Aviation Administration (FAA). The commenter sought clarification that new requirements, including incident reporting requirements, would not apply to systems that are under the port authority's charge but that are unrelated to maritime port activities. The commenter expressed concern that, if the Coast Guard rule were to apply to all systems under a port authority's charge, many ports would have dual reporting requirements for the same incidents—a significant inefficiency.

This final rule is applicable to those facilities currently regulated under existing MTSA regulations. By and large, airport facilities are not regulated under this rule. If a situation arose where a MTSA-regulated entity was potentially subject to conflicting requirements from the Federal Aviation Administration—or any other agency's requirements—the entity should raise the issue of any perceived conflicts with the COTP and that agency's respective point of contact so that each agency is aware of the concern and can evaluate if there are conflicts for compliance. With respect to incident reporting, if there are occurrences where a cybersecurity incident affects systems or equipment falling under multiple regulatory jurisdictions, an owner or operator will have to ensure all reporting requirements are met. And with respect to the rule in general, if appropriate, the Coast Guard, acting through the COTP, may recommend the entity consider a request for equivalence in order to avoid overlapping requirements.

Some commenters stated that the United States should not impose specific requirements for the flag state on its vessels without imposing the same on foreign-flagged vessels. One commenter also suggested that U.S.-flagged vessels should be subject to requirements no greater than those applied to foreign-flagged vessels with a safety management system. The commenter asserted that, once the IMO establishes international requirements, a new NPRM should be issued to implement these requirements for U.S.-flagged vessels. Other commenters said the United States should not impose requirements that deviate from international standards, including those

[42] See FEMA, ''The U.S. Department of Homeland Security (DHS) Notice of Funding Opportunity (NOFO) Fiscal Year 2024 Port Security Grant Program,'' April 16, 2024, *https://www.fema.gov/print/pdf/node/676012,* accessed October 23, 2024.

[43] Id. at 14.

[44] Id. at 6.

[45] Pub. L. 115–254, Div. J.

that are presently being negotiated at the IMO.

The Coast Guard believes that protecting U.S. national security and the nation's sovereign interests is a paramount concern. As the flag administration, the United States believes that these baseline requirements for U.S.-flagged vessels are important preventive measures. Not only will establishing these requirements help protect the U.S. commercial fleet from cybersecurity threats, but it will also further establish the United States as a leader in this space and offers a model for the necessary actions that other flag administrations should take with respect to the cybersecurity of vessels.

The Coast Guard acknowledges that this final rule adds new requirements on U.S.-flagged vessels. However, the Coast Guard believes that proactive cybersecurity regulations are essential for ensuring the continued safety, security, and resilience of the domestic MTS. Consistent with this approach, the United States is actively engaged in international efforts to address maritime cybersecurity at the IMO. The Coast Guard believes that extending regulations to foreign-flagged vessels at this time while these discussions are ongoing would disrupt the established processes for port state control and possibly jeopardize U.S. national interests. The Coast Guard may consider revising this rule at a later date as the threat environment and international standards develop, including after the IMO speaks to cybersecurity with additional specificity.

Multiple commenters requested clarification on how these regulations apply to existing U.S.-flagged vessels, facilities, and OCS facilities, and stated that it could be difficult for existing vessels to meet some requirements. Specifically, concerns were raised about the inability to implement data encryption, the feasibility of compliance with network segmentation, frequent operator changes, difficulty in identifying personnel to fill a specialized position, and the presence of minimal computer networks and electronic systems. One commenter stated that vessels operating exclusively on inland waters, such as barges and towing vessels, have a minimal cyber footprint and should be excluded from this rulemaking.

This final rule is applicable to U.S.-flagged vessels, facilities, and OCS facilities, and includes both existing U.S.-flagged vessels, facilities, and OCS facilities, as well as any new or future U.S.-flagged vessels, facilities, and OCS facilities. The Coast Guard understands that IT and OT footprints can vary across vessels. As discussed in Section VII of this preamble, for the reasons indicated below, the Coast Guard requests public comment on a potential 2-to-5-year delay for the implementation periods for U.S.-flagged vessels, which may partially address the commenters' concerns about vessels. Conducting the required Cybersecurity Assessment allows for regulated entities to determine and not merely speculate about their specific IT and OT footprint, including potential vulnerabilities. Even vessels with a small IT or OT footprint may still face cybersecurity risks that could impact operations, safety, and security, which must then be addressed. Some such limitations may be addressed in the Cybersecurity Plan. When a regulated entity believes that certain requirements are not applicable or they are unable to comply with specific requirements within this regulation, they may follow the procedures in § 101.665 to request a waiver or equivalency.

While the Coast Guard recognizes that issues such as frequent operator changes may result in additional work for a regulated entity, this final rule is in line with existing requirements applicable to owner or operator changes. The Coast Guard believes that cybersecurity training remains crucial for safeguarding the MTS against evolving cybersecurity threats. Each new operator introduces a potential vulnerability, and, without adequate training, this could compromise both IT and OT systems. To mitigate these risks, it is vital that all operators, regardless of turnover frequency, are equipped with fundamental cybersecurity knowledge and skills. While formal training may be appropriate, the Coast Guard is not mandating a format of training in this final rule. 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. When a regulated entity believes they are unable to comply with specific requirements within this regulation, they may follow the procedures in § 101.665 to request a waiver or equivalency.

Some commenters suggested that the Coast Guard should create a separate rulemaking for vessels.

The Coast Guard is not considering a separate rulemaking for vessels at this time. This final rule is consistent with the Coast Guard's authority under MTSA as it applies to vessels.

Some commenters asked that this final rule not apply to vessels such as small passenger vessels, towing vessels, and barges, as well as to facilities with minimal or no IT and OT footprint. One commenter stated that the NPRM outlined cybersecurity procedures broadly applicable to many vessels and facilities but failed to consider those with minimal computer networks and systems that would not significantly impact operations, security, or safety if compromised. Another commenter stated that OT systems on vessels are distinct and should be assessed separately from shoreside infrastructure, as cyber incidents typically impact only one vessel at a time due to segmentation. In contrast, shoreside incidents can have wider repercussions. For inland vessels, the primary vulnerabilities are personally identifiable information (PII) and positional data theft. Thus, the commenter recommended a tiered risk system to determine suitable cybersecurity measures for vessels.

The Coast Guard does not agree with changing the applicability of this final rule. Developing a definition or standard for ''little or no IT and OT footprint'' would be challenging, and the Coast Guard did not seek comment on such a definition in this rulemaking. Moreover, the Coast Guard is not aware of a definition for ''little or no IT and OT footprint'' in other regulations or in other recognized standards.

Until an Assessment is completed, it would be difficult to know the full extent of a regulated entity's IT and OT footprint, and even a smaller IT and OT footprint could still allow cybersecurity threats and vulnerabilities and could still result in a cyber incident. It is necessary for all regulated entities under this final rule to first conduct the required Cybersecurity Assessment to determine the extent of their IT and OT footprint. Upon completion of that assessment, each regulated U.S.-flagged vessel, facility, or OCS facility can then develop a Cybersecurity Plan based on the applicable requirements. Even if an Assessment identifies only a minimal IT and OT footprint, that footprint may still represent levels of risk to the owner or operator, as well as the MTS. If the owner or operator finds there are portions of these regulations that do not apply to their U.S.-flagged vessel, facility, or OCS facility, the Coast Guard offers procedures in § 101.665 for an owner or operator to request a waiver or equivalence determination for the requirements. While an item may be identified by an owner or operator as not applicable, and therefore requires a waiver request from the requirement, it is necessary to identify that through the Cybersecurity Assessment and

document in a Cybersecurity Plan so that it can be reviewed in the future as needed.

Multiple commenters recommended the Coast Guard coordinate with the Bureau of Safety and Environmental Enforcement (BSEE) in the Department of the Interior before issuing any cybersecurity requirements for OCS facilities because of the shared authorities in OCSLA.

The Coast Guard and BSEE have a shared mission of ensuring safety on the OCS. We work closely together to ensure our requirements are not in conflict with each other. The Coast Guard will continue to work with BSEE and our other interagency partners to harmonize efforts as appropriate and according to OCSLA and any other applicable law.

One commenter requested clarity about applicability to §§ 104.105(b) and 105.105(b).

The Coast Guard revised the language in § 101.605 to clarify that these cybersecurity regulations apply to the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under parts 104, 105, and 106. The text ''required to have a security plan'' is the clearest means to clarify the applicability without the loss of legal precision, especially as MTSA addresses regulated entities in a similar manner at 46 U.S.C 70103.

The Coast Guard received multiple comments suggesting that the applicability for these requirements should be a risk-based approach based on the varied levels of IT and OT footprints, or how extensive a cybersecurity incident would be, based on vessel, facility, or OCS facility size and type of operation, including a consideration for the applicability to U.S. domestic vessels. Multiple commenters contended that prescribing the same requirements for all vessels and not scaling the applicability of requirements based on risk profile would impose unfeasible requirements and undue burdens on owners and operators of vessels. One commenter indicated that this risk-based approach should also apply to penetration test requirements. Another commenter further suggested that the Coast Guard add objective criteria for cybersecurity controls similar to what is currently addressed in NVIC 01–20.

The Coast Guard determined that these cybersecurity requirements should apply to the same entities to which MTSA currently applies, but that there are areas where a waiver under § 101.665 could apply. The Coast Guard would not currently be able to identify the unique aspects of each vessel and facility to develop a comprehensive risk factor system and base requirements off that. Additionally, risk factors could change, so the Coast Guard would either risk developing factors that become outdated, or otherwise could not keep up with a changing IT and OT landscape. The Coast Guard feels that the best approach is to develop a broad range of cybersecurity requirements in this final rule, which serve as baseline requirements across all regulated entities rather than a risk-based approach. Since each individual entity will have unique features, including their IT and OT footprint, we believe it makes the most sense for them to assess themselves, and, if needed, identify where they cannot comply or when a requirement is not applicable.

It is practical to maintain the existing MTSA applicability, particularly in requiring those regulated stakeholders to complete a Cybersecurity Assessment to identify the extent of their IT and OT footprint, so all entities can determine which requirements under these regulations would apply. In cases when an owner or operator determines, through their assessment, that certain criteria do not apply, they may follow the procedures in § 101.665 to request a waiver or equivalency. NVIC 01–20 serves as general guidance for incorporating cybersecurity into existing FSA and FSP requirements in 33 CFR part 105. This final rule represents more comprehensive cybersecurity requirements that go beyond those addressed by NVIC 01–20. An owner or operator may, however, use the principles of NVIC 01–20 to help inform their compliance with these regulations.

One commenter suggested that the Coast Guard revise § 101.605 so that this final rule would not apply to a vessel or facility that has not installed an IT or OT system that, if compromised, could result in a TSI. The commenter also suggested that the Coast Guard modify 33 CFR 104.305 and 105.305 so that VSAs and FSAs require an analysis of cybersecurity threats as defined in § 101.615.

The Coast Guard does not agree with this recommendation as we are not making changes to existing regulatory requirements in 33 CFR parts 104 and 105. In addition, the recommendation to revise 33 CFR part 101 would introduce too much uncertainty into applicability, especially as it relates to the need for entities to conduct a Cybersecurity Assessment to evaluate risks as a threshold matter. It would be premature to carve-out a regulated entity based on an assumption the regulated entity's IT or OT poses no risk to the MTS or risk of TSI before such an evaluation is made through a Cybersecurity Assessment. The function of the Cybersecurity Assessment is to provide the necessary information to develop the appropriate mitigation measures within the Cybersecurity Plan and to provide the substance that would inform any discussions with the COTP or MSC, especially as it may relate to requests for waivers or equivalencies.

One commenter requested clarification as to the applicability of these regulations in cases of a landlord port and tenant facilities.

These regulations create new baseline cybersecurity responsibilities for the owner or operator of an applicable U.S.-flagged vessel, facility, or OCS facility. ''Owner or operator'' is a term defined at 46 U.S.C. 70101(5). The applicability of these regulations may depend on the nature of any specific landlord port and tenant facility agreements. Therefore, the Coast Guard cannot make a blanket determination about all landlord-tenant relationships as it relates to the responsibility for compliance with the requirements of this final rule.

Some commenters suggested that the Coast Guard incorporate these rules into the existing 33 CFR parts 104, 105, and 106 requirements, as opposed to creating 33 CFR subpart F.

The Coast Guard considered this approach but determined that putting these cybersecurity requirements in a single subpart within 33 CFR part 101, which would then follow the applicability of 33 CFR parts 104, 105, and 106, allowed for the best alignment across regulated entities. The Coast Guard has chosen to articulate the cybersecurity requirements within 33 CFR part 101 because these regulations impact U.S.-flagged vessels, facilities, and OCS facilities collectively. This format is presented in a more organized and accessible manner to the maritime partners who are already familiar with the MTSA regulations.

Some commenters asked us to clarify whether 33 CFR subpart F will supersede NVIC 01–20.

NVIC 01–20 is a guidance document that states the Coast Guard's policy stance and an interpretation of its existing regulations. NVIC 01–20 itself is not enforceable as a legislative rule. The cybersecurity guidance provided by NVIC 01–20 relates to the requirements in 33 CFR part 105 that predate this rulemaking. Upon the effective date of this final rule, the requirements in these regulations will have the force of law. This final rule will supersede NVIC 01–20.

Some commenters raised concerns that some stakeholders will be affected

by limited workforce and resources and questioned the cybersecurity benefits. The commenters asserted that these challenges would be a significant hindrance to operational effectiveness and urged the Coast Guard to provide sufficient time and flexibility for operators to understand and implement the new requirements. The Coast Guard recognizes that regulated entities will have different workforce levels, as well as financial and other resources, that affect how they will comply with this final rule. In many cases, regulated entities with a smaller workforce and fewer resources will likewise have a smaller IT and OT footprint to assess and address in a Cybersecurity Plan. If those entities do have a large IT and OT footprint, then that reinforces the need to comply with the requirements in this final rule to prevent, mitigate, and respond to cybersecurity threats, vulnerabilities, and incidents.

One commenter stated that this final rule had an unclear impact on marine terminal operators participating in unified port authority cybersecurity programs.

The Coast Guard encourages participation and collaboration between stakeholders and maritime entities in addressing cybersecurity and other security risks throughout a port complex. However, a unified port authority cybersecurity program or similar higher-level arrangement may not adequately account for the unique cyber threats and vulnerabilities for a specific regulated entity. This final rule represents requirements for each regulated U.S.-flagged vessel, facility, and OCS facility, consistent with existing security requirements according to 33 CFR parts 104, 105, and 106.

The Coast Guard believes that both this final rule and unified port authority cybersecurity programs can work in complement to each other, as they both pursue the same goal of bolstering cybersecurity, where the port authority program can be viewed as a macro-level plan, rather than the micro-level, individualized plan specific to the U.S.-flagged vessel, facility, or OCS facility. This final rule is based on CISA's CPGs, which themselves are informed by NIST's Cybersecurity Framework (CSF), and all leverage commonly accepted cybersecurity best practices that should not conflict with other programs. This final rule represents minimum baseline standards that a regulated entity can further build upon in coordination with unified port authority cybersecurity programs.

Many ports have an active and robust AMSCs, which may include a Cybersecurity Subcommittee that can address coordination. Since this final rule and unified port authority cybersecurity programs all share a common goal of ensuring cybersecurity, the Coast Guard expects that regulated entities and port authorities will work together to ensure programs are not in conflict. Additionally, in cases when a unified port authority cybersecurity program may impact a regulated entity's specific cybersecurity plan, and owner or operator may be able to address the impact through the provisions in § 101.665 for noncompliance, waivers, and equivalents.

C. Comments Related to Definitions

Sources for Definitions Used in This Final Rule

Some commenters suggested using definitions for certain terms used in this final rule that come from sources such as NIST, DoD's Cybersecurity Maturity Model Certification program, and other standards.

The Coast Guard selected the definitions used in this final rule based on definitions used by our interagency partners to ensure alignment and harmonization across the interagency. The NPRM [46] discussed the citations for these definitions. The Coast Guard recognizes that there are numerous definitions for many of the terms used in this final rule, and that many might choose other sources, but these definitions meet the needs of the Coast Guard and are overwhelmingly accepted by stakeholders. The definitions used here are standard cybersecurity definitions used across industry and Government agencies and are listed in NIST's CSF. This common lexicon helps limit miscommunication.

Harmonizing Definitions

One commenter noted that harmonization of definitions for existing and proposed cybersecurity requirements is vital.

As discussed in the preamble of the NPRM, the Coast Guard consulted numerous sources for the definitions used in the NPRM. These sources include Executive Order 14028, the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 (Pub. L. 117–263) (the Act), the Homeland Security Act of 2002 (Pub. L. 107–296), as amended, CISA's National Initiative for Cybersecurity Careers and Studies, and NIST's Computer Security Resource Center (CSRC). We believe that these sources are reliable and generally accepted by the industry and Government agencies. Additionally, these terms are appropriate for usage in the maritime setting. The definitions used here are standard cybersecurity definitions used across industry and Government agencies and are listed in NIST's CSF. However, we also recognize that there is some variance in the cybersecurity terms used by industry and Government sources. For example, NIST defines a ''cyber incident'' as ''an occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.'' Part 6 of title 33 of the CFR uses similar, but not identical, language to define a cyber incident as an occurrence that:

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.[47]

The Homeland Security Act of 2002 also uses similar language, defining an incident as ''an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.'' [48]

After reviewing all these definitions, we selected the ones that best fit the maritime setting and ensured that the regulatory definitions are consistent with the relevant statutory definitions. The definitions used here align with standard cybersecurity definitions used across industry and Government agencies and are listed in NIST's CSF. These sources provide a common lexicon for everyone to use to limit miscommunication and do not differ because they are used in a maritime setting.

Adding New Terms to the Final Rule

Several commenters suggested that we introduce new terms that were not defined in the NPRM, such as ''Marine Transportation System (MTS),'' ''Critical Cybersecurity Equipment,'' and ''transportation security incident.'' In some cases, commenters proposed adding new definitions to enhance understanding of this final rule. For

[46] 89 FR 13404.

[47] 33 CFR 6.01–8 and 44 U.S.C. 3552(b)(2).

[48] 6 U.S.C. 650(12).

example, they requested definitions for ''key personnel'' as described in § 101.650(d), Cybersecurity Training for Personnel, and ''sensitive or critical data'' instead of the current requirement that ''all data'' must be protected under § 101.650(c), Data Security Measures. The commenters noted that these suggestions were made to clarify specific requirements and improve the overall clarity and implementation of this final rule.

We did not make changes in response to most of these suggestions. Adding these terms is unnecessary, as many of them are already well-defined and have been commonly used in the maritime sector for many years. For example, ''Marine Transportation System'' or ''Maritime Transportation System'' are terms that are widely recognized and understood by industry and Government agencies.[49] Similarly, transportation security incident is a term that, although mentioned several times in the NPRM, was not defined because it is already defined at 46 U.S.C. 70101 and in 33 CFR 101.105. This definition has been in place for over 20 years under the MTSA regulations. Therefore, we do not see the need to introduce additional definitions for these terms.

Some commenters suggested that the Coast Guard define what is a ''significant number'' when disclosure or unauthorized access directly or indirectly of nonpublic personal information of individuals information requires reporting in the proposed definition for reportable cyber incident.

The Coast Guard did not make changes in response to these requests. We recognize that we use several terms, such as ''significant number,'' in this final rule without defining them. We intentionally left this and other terms undefined because their meanings can vary significantly depending on an organization's operational conditions and cybersecurity risks. This approach ensures that the definition is appropriately tailored to the unique context and needs of each organization. By allowing organizations to define these terms themselves, we aim to provide a more flexible approach to meet the requirements in the evolving cybersecurity environment in the maritime sector.

Defining the Term ''Reportable Cyber Incident''

Numerous commenters responded affirmatively to our request for comments on whether we should define and use the term ''reportable cyber incident'' in this rulemaking to clarify what incidents trigger reporting obligations. Some commenters offered suggestions on edits to this proposed definition, including reordering subparagraphs. One commenter suggested limiting the definition to known incidents and not including those still under investigation considering the DHS report, informed by the work of the Cyber Incident Reporting Council (CIRC), which advises that the Federal Government should adopt a consistent model definition of a ''reportable cyber incident'' wherever practicable. Another commenter noted that establishing a threshold for reportable cyber incidents based on the potential that the incident could result in a TSI would clarify what does and does not need to be reported. Another commenter recommended that the Coast Guard should narrowly tailor ''reportable cyber incident'' to align with the Coast Guard's mission and the underlying purpose of the MTSA.

The Coast Guard agrees with the suggestion to define and use the term reportable cyber incident. We have included the term reportable cyber incident in this final rule. The Coast Guard's definition of reportable cyber incident is based on the model definition proposed in the CIRC-informed DHS Report (the ''CIRC Model Definition'').[50] Interagency stakeholders reviewed this term and its definition to ensure alignment and harmonization to the extent practical. The Coast Guard did not adopt the suggested edits to the proposed definition. We are maintaining the definition we included in the preamble to the NPRM, based on other public comments and discussion with interagency partners on harmonization.

One commenter stated that the definition for reportable cyber incident should include clearly defined thresholds for such incidents.

The Coast Guard does not agree. The definition for a reportable cyber incident provides sufficient detail to allow owners, operators, or CySOs to determine what constitutes such an incident and reflects harmonization among the interagency on the substance of this definition.

As noted previously, after considering all public input, we have decided to include the term reportable cyber incident as defined in the NPRM. We concur with the many comments that this term is sufficiently well-defined to provide clear guidance on when and under what conditions cyber incidents must be reported to the NRC. This clarity will help eliminate the need to report minor cyber incidents, which will reduce the administrative burden on owners and operators as a result.

One commenter suggested that the Coast Guard include the definition for a reportable cyber incident, but to allow for a threshold that would include unauthorized attempts by third-party actors to access sensitive information. The commenter also stated that these incidents should include phishing attempts, attempts to gain access to terminal operating systems, and unsuccessful malware attacks, as well as loss of network availability, exposure of sensitive data, and disruption of business operations as a result of unauthorized access by third parties.

We did not adopt this suggestion. The Coast Guard's definition allows for the owner, operator, or CySO to determine if an incident meets the criteria for reporting. Further, the Coast Guard encourages stakeholders to report any situation or incident out of the ordinary if there is doubt or if they question whether it meets the definition of reportable cyber incident.

We acknowledge the concerns raised by some commenters about redundancy and the need for interagency coordination. The Coast Guard will continue to work with other Government agencies to ensure our language aligns among all regulations and ensure harmonization of efforts to the extent practicable.

The Coast Guard emphasizes information sharing among its interagency partners. The Coast Guard shares information with other Federal agencies through multiple channels: NRC reports of incidents are shared with DHS, CISA, and other relevant agencies. As a Co-Sector Risk Management Agency for the Transportation Systems Sector, the Coast Guard regularly communicates with the U.S. Department of Transportation, the Maritime Administration, TSA, and CISA.[51] The Coast Guard is a participant on numerous National Security Council-led Interagency Policy Committees. Engagement among local, State, Federal, and Tribal agencies also occurs through AMSCs. The Coast Guard shares cyber-focused products such as marine safety

[49] *See* for example, 46 U.S.C. 50401.

[50] *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 August 13, 2024.

[51] The White House, National Security Memorandum on Critical Infrastructure Security and Resilience, Apr. 30, 2024, *https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/,* accessed on December 20, 2024.

information bulletins, cyber advisories, and other products across interagency partners.

One commenter noted that they support defining reportable cyber incident to distinguish between incidents that must be reported and those that do not; however, they find the current definition of ''cyber incident'' in § 101.615 is too broad and overly focused on IT. The commenter also noted that they have concerns with the proposed definition of reportable cyber incident and its alignment, or lack thereof, with other definitions for reportable cyber incidents in regulation and policy.

The Coast Guard definition of cyber incident is based on the existing definition of incident in Title XXII of the Homeland Security Act of 2002,[52] which is not textually identical, but is substantively similar in relevant part to, the definition of ''cyber incident'' in Executive Order 14116. An incident in the Homeland Security Act of 2002 is ''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.'' Although the Coast Guard recognizes that not all commenters may agree with our chosen definition, the Coast Guard values alignment with these established terms to minimize potential conflicts that could be created by significant deviations between definitions in these regulations and existing statutes.

''Information system'' is defined in this final rule as an interconnected set of information resources under the same direct management control that shares common functionality. Typically, a system includes hardware, software data, applications, communications, and people. It includes the application of IT, OT, or a combination of both. The definition of information system clearly covers both IT and OT systems.

The Coast Guard's definition of reportable cyber incident is based on the model definition proposed in the CIRC Model Definition. However, in CISA's proposed rule implementing the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (Pub. L. 117–103), the proposed definition of ''substantial cyber incident'' (which is used within the definition of ''covered cyber incident,'' the term that describes what cyber incidents are required to be reported under CIRCIA) does not include the CIRC Model definition's phrase ''or, if still under the covered entity's investigation, could reasonably lead to any of the following,'' as CISA interprets CIRCIA to require an incident to actually result in one of the impacts listed in the definition of substantial (in this case, reportable) cyber incident under CIRCIA.[53] For similar reasons, CISA did not propose including in the definition of ''substantial cyber incident,'' the CIRC Model Definition's fourth threshold prong, ''potential operational disruption.'' A ''reportable cyber incident'' is a type of ''cyber incident'' as these terms are defined in this final rule. A ''reportable cyber incident'' as defined in this final rule would also trigger a reporting obligation under 33 CFR 6.16–1 for entities required to report a cyber incident as such term is defined in 33 CFR part 6.

Revising the Definition of ''Breach''

One commenter noted that the term ''breach,'' when used by the Coast Guard to discuss a breach of security, could have serious, significant legal and financial impacts in reference to cybersecurity.

We revised § 101.625(d)(10) in this final rule to refer to ''reportable cyber incidents'' rather than ''breaches of security, suspicious activity that may result in TSIs, TSIs, and cyber incidents.'' This is also consistent with our decision to define and include the term reportable cyber incident.

Adding a Definition for ''Cybersecurity Threat''

One commenter recommended adding the definition of ''cybersecurity threats'' to 33 CFR parts 104 and 105.

The Coast Guard does not agree to add the definition of ''cybersecurity threat'' because it is already encompassed by the defined term ''cyber threat'' the Coast Guard uses in this final rule. Cyber threat is the term used in CIRCIA, which amended the Homeland Security Act of 2002 (Pub. L. 107–296). CIRCIA defined cyber threat by cross-referencing to the term cybersecurity threat as it was already defined in the Homeland Security Act of 2002. The two statutory terms share the same definition, which is substantively repeated in this final rule. For the sake of consistency in this final rule, the Coast Guard has chosen cyber threat as the term-of-art for these regulations.

Furthermore, the Coast Guard does not concur with the suggestion to amend 33 CFR parts 104 and 105 because, except for amending 33 CFR 160.202, this final rule is limited to establishing requirements in 33 CFR part 101. Adding or removing requirements in parts 104, 105, or 106 is outside the scope of this final rule. The new definitions in § 101.615 are sufficient for this final rule.

Revising the Definition of ''Backup''

One commenter raised a concern that the primary issue with the concept of ''backup'' is that it lacks the flexibility to rebuild or re-instantiate a system from something other than a backup. When restoring from backups, time can be a critical factor. Therefore, the commenter recommended that the Coast Guard expand this definition and eliminate the requirement for all backups to be stored offsite.

The Coast Guard agrees with this commenter. We revised the definition of backup in § 101.615 to remove the phrase ''in a secondary location'' and the implication that backups must be stored ''offsite.'' Instead, we added language to clarify our definition of backup. In this final rule, backups refer to ''copies being stored separately for preservation and recovery.'' With these changes, the revised definition is sufficient for the requirements in these regulations. If an owner or operator of a U.S.-flagged vessel, facility, or OCS facility identifies a method that they feel falls outside of that definition, they may follow the process to request a waiver according to § 101.665.

Defining the Term ''Transportation Security Incident''

One commenter questioned the clarity of the definition of a ''transportation security incident,'' while another suggested a definition of ''security incident.''

Transportation security incident is defined by the MTSA, codified at 46 U.S.C. 70101, and in 33 CFR 101.105. Further guidance on what constitutes a TSI (as well as a ''breach of security'' or ''suspicious activity'') is provided in NVIC 02–24.

Revising the Definition of ''Hazardous Condition''

Multiple commenters addressed our request for input on whether we should amend the definition of ''hazardous condition'' in 33 CFR 160.202 by adding ''cyber incidents.'' The Coast Guard received several comments in favor of amending the definition of hazardous condition to include cyber incidents. Conversely, one commenter advised against including cyber incidents under the definition of hazardous condition in § 160.202. The commenter warned that doing so could lead to unnecessary sharing of sensitive information during

[52] Public Law 107–296, as added by Public Law 117–263, section 7143, classified to 6 U.S.C. 650.

[53] 89 FR 23644.

cyber incidents, such as losing confidential data, that do not impact marine operations. The commenter recommended against additional reporting requirements beyond those mandated by CISA if cyber incidents are added to the definition of hazardous condition. Other commenters also suggested that the Coast Guard clarify the application of this definition to marine terminals and OCS facilities, as much of this section pertains to vessel requirements and may cause confusion.

The Coast Guard concurs with the recommendations to include the term. Accordingly, we amended the definition of hazardous condition in that section to include the term cyber incident. Including the term cyber incident is a helpful example that adds clarity to the existing regulation in 33 CFR 160.202, which applies only to vessels. The Coast Guard recognizes that not all occurrences with a cyber aspect will create a hazardous condition, but believes the term's inclusion in the list of examples will be beneficial by highlighting that cybersecurity is an important consideration that operators should be cognizant of when assessing hazardous conditions.

As discussed elsewhere in this preamble, the Coast Guard amended the definition of hazardous condition to include cyber incidents. The Coast Guard is not changing the applicability of § 160.203 to include facilities or OCS facilities because § 160.203 relates to the Notice of Arrival and Departure regulations for vessels. This clarification to the definition of hazardous condition is distinct from the new baseline cybersecurity requirements for MTSA-regulated entities.

One commenter expressed concern with the NPRM's approach to requesting input on whether to define and use reportable cyber incident, and whether to amend the definition of ''hazardous condition.'' The commenter strongly advocated for harmonizing the reporting process, noting that owners and operators of U.S.-flagged vessels are already familiar with reporting to the NRC. They suggested that all cyber incidents should be reported through this channel, allowing the NRC to relay information to other Federal agencies as needed.

The Administrative Procedure Act requires that we provide general notice of a proposed rulemaking, including notice of the terms or substance of a proposed rule or a description of the subjects and issues involved.[54] Asking the public to comment on specific items, in addition to the NPRM as whole, is a commonly accepted way to seek public participation in the rulemaking process. In fact, as discussed above, we received numerous comments responsive to our request.

D. Comments Related to Owner or Operator

We received a series of comments about the responsibilities of the owner or operator for managing the Cybersecurity Plan.

One commenter recommended assigning responsibilities to the operator to ensure compliance with applicable regulations for regulated facilities. One commenter recommended assigning overall responsibility for vessels to the company or organization (in this case, a Document of Compliance (DOC) holder) if the owner and operator of a vessel are separate entities. Another commenter recommended the term ''owner and operator'' be clarified to signify a single responsibility for the vessel (in this case, a DOC holder), OCS facility, or other facility owned or operated, based on IMO practice.

We did not make changes in response to these recommendations. The Coast Guard desires consistency with the existing regulations and uses the term ''owner or operator'' as defined in § 101.105 throughout this final rule. The Coast Guard does not agree that further clarification of the term ''owner or operator'' is needed. The term owner or operator in this final rule is consistent with existing MTSA regulations, and it is unnecessary to specify further criteria for the entity with overall responsibility (such as requiring them to be holding a DOC).

One commenter requested clarification of the differences between the roles and responsibilities of the owner or operator and the CySO as there are similar or overlapping roles to both.

The roles and responsibilities of the CySO and owner or operator are clearly outlined in this final rule in §§ 101.625 and 101.620, respectively, and are in line with the existing relationships between the owner or operator, Vessel Security Officer (VSO), and Facility Security Officer (FSO) in existing regulations. While there is some overlap between the roles, any redundancy or overlap does not take away from the responsibilities of the CySO and owner or operator and enables the owner or operator to maintain oversight over the CySO position.

One commenter recommended that the Coast Guard change the phrase ''responsible for'' to ''accountable for'' in § 101.620(a) when referring to owners and operators assigning security duties to other personnel. According to the commenter, this change would highlight the importance of how these roles will be staffed and implemented, indicating a more structured approach to accountability within the organization.

The Coast Guard declined to make this change, as the term ''responsible for'' is consistent with existing language for VSOs, FSOs, and OCS FSOs in current regulations and is long-standing industry practice.

One commenter questioned whether ''person'' as stated in § 101.620(b)(2) is synonymous with ''role.''

An owner or operator subject to this final rule is required to identify each person exercising cybersecurity duties and responsibilities. Any person having such duties and responsibilities would likewise have a ''role.'' Owners and operators should focus on the language of this final rule and identify each person, as stated. The Coast Guard is concerned that the necessary duties are properly assigned and performed. The particular manner which an entity identifies and assign those duties, whether by individual name or by role, is left to the entity's discretion. The Coast Guard encourages owners and operators to comply with the requirements under § 101.620(b)(2) consistent with how their U.S.-flagged, facility, OCS facility, or organization addresses similar requirements in their VSP, FSP, or OCS FSP.

E. Comments Related to Cybersecurity Officer

Some commenters stated that they did not believe that cybersecurity warrants another designation for security personnel, in this case a CySO, and felt that a specific cybersecurity plan was not needed. They recommended adding cybersecurity duties to existing responsibilities of the Company Security Officer (CSO) and VSO. Another commenter felt that the CySO position might be unnecessary and requested a process for waiving this requirement. Another commenter believed that this final rule should state the actions that an organization must take, rather than specifying the individual role that needs to accomplish those actions. They felt that organizations should be able to identify who that person would be for their organization, which may align to other positions or titles within their organization.

The Coast Guard strongly believes that the present and evolving cybersecurity threats in the MTS require specific regulations to help prevent, mitigate, and respond to cybersecurity incidents and vulnerabilities. This final rule provides minimum cybersecurity

[54] 5 U.S.C. 553(b)(3).

requirements for a common cybersecurity baseline for regulated maritime entities. The threats and vulnerabilities addressed are not adequately covered by existing regulations. The requirements to designate a CySO and to develop a Cybersecurity Plan reflect the reality that cybersecurity threats, risks, and vulnerabilities exist in the MTS, and have the potential to significantly affect the safety and security of individual entities, as well as the MTS and other transportation critical infrastructure. The Coast Guard has determined that it is necessary to identify a specific CySO, similar to the identification of a VSO or FSO, that serves as the primary lead to organize these efforts within their U.S.-flagged vessel, facility, or OCS facility, to ensure that there is at least one representative focusing on and addressing the relevant requirements. Consistent with § 101.625, the CySO may perform other duties such as CSO, FSO, or VSO. It will be up to owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to decide whether they need to designate a sole security officer that focuses exclusively on cybersecurity.

One commenter stated that the requirements for cybersecurity should be directed at the executive level, and not create a CySO position to handle many of these requirements.

The owner or operator has ultimate responsibility for compliance with this final rule. This includes the designating a CySO, as required by § 101.620(b)(3). It is the responsibility of each regulated entity to ensure their executive leadership is aligned with the CySO and other cybersecurity professionals. Placing full ownership of cybersecurity requirements on the owner or operator, without the designation of a CySO, would be burdensome to the owner or operator. The position of CySO ensures the regulated entity has personnel with the necessary professional expertise to address cybersecurity.

Several commenters stated that the qualifications listed in these regulations did not fully encompass what would be required for a successful CySO position. Additionally, a commenter questioned the qualifications of the Coast Guard or a third-party organization to evaluate what is required of a specific organization's CySO. The commenter also suggested that either the Coast Guard or a third-party organization would be in a poor position to evaluate whether they meet the necessary qualifications. Another commenter stated that it could be difficult for small organizations to have someone on staff with these qualifications.

This final rule presents minimum baseline requirements, including the requirements of a CySO for a U.S.-flagged vessel, facility, or OCS facility. The qualifications required serve as a baseline that should be attainable and easily evaluated by organizations of any size or complexity. Organizations are welcome to identify additional requirements, such as additional qualifications, that they would require of their CySO position as best suits their individual needs, so long as the minimum requirements of this final rule are met. It is up to the owner or operator of a U.S.-flagged vessel, facility, or OCS facility to determine that their candidate meets these requirements, and for the Coast Guard to evaluate whether the owner or operator met their required responsibilities in their review of the Cybersecurity Plan.

The Coast Guard does not, and will not, have a role in an organization's hiring of new personnel or designation of new roles and responsibilities to existing personnel. These decisions are left up to the owner or operator. The Coast Guard has stated that the CySO can be an existing employee at a U.S.-flagged vessel, facility, or OCS facility. The Coast Guard will verify that a qualified CySO has been designated by the owner or operator according to this final rule. The Coast Guard recognizes that this final rule will result in costs incurred by industry. Failure to designate a CySO, as well as failure to comply with any other aspect of this final rule, would be subject to actions as determined by the COTP or other appropriate Coast Guard representative.

One commenter asked the Coast Guard to clarify if the CySO must be a U.S. citizen.

The Coast Guard does not impose citizenship requirements for the CySO position in this final rule. The Coast Guard may consider this issue in a subsequent rulemaking, as appropriate.

Some commenters noted that for small operators, or those with limited resources, the CySO would likely be a collateral duty. Another commenter similarly commented that it was not reasonable to expect every owner or operator of a vessel to employ a cybersecurity expert, and that the CySO position requires too much specialized knowledge and too much time to be added to an existing position. Many small companies without an in-house IT department might have to rely on a third-party provider for all cybersecurity needs and protections. Consequently, the commenters were concerned that this final rule would impose unrealistic requirements and undue burdens on small operators. Some commenters requested that the Coast Guard clarify that a CySO could be someone designated at the corporate level.

The Coast Guard notes in this final rule that the CySO designation may be given to an employee with other responsibilities consistent with § 101.625. The CySO role may be a collateral duty so long as all the requirements and responsibilities of the position are met. It is the responsibility of owners and operators to ensure that cybersecurity risks are managed and addressed, whether through in-house resources or through third-party services. While we understand the concerns regarding the potential burden of compliance, it is essential that cybersecurity requirements are met to safeguard the organization's assets and ultimately, maritime critical infrastructure and the MTS. Ensuring robust cybersecurity defenses is critical to protecting against potential threats and maintaining operational integrity.

The Coast Guard developed these regulations, including the cybersecurity requirements, to enable owners and operators to identify a person who can manage the requirements, even if they must rely on other cybersecurity, IT, or OT professionals for more technical items in the rule. Regardless of the size of an organization itself, the size of their IT and OT footprint dictates how much a CySO will have to address. A company with a small IT or OT footprint would likewise be scaled towards fewer items that the CySO would be responsible for. A company with a larger IT or OT footprint would similarly require more of the CySO position, commensurate to the level of risk posed. The Coast Guard believes, therefore, that there would be little to no undue burden or unrealistic requirement of any regulated entity, as the level of cybersecurity actions required of the CySO directly correlates to their cyber footprint. The Coast Guard reiterates that this final rule allows for the designation of the CySO role to an existing employee at any level of the organization, so long as the requirements and responsibilities are met for each individual U.S.-flagged vessel, facility, or OCS facility.

Some commenters requested that the Coast Guard recognize that a facility may designate an alternate CySO. Their concern is that, for a company with multiple facilities, one CySO may not have the knowledge or practical capability to effectively manage all of them.

The Coast Guard revised the definition for *Cybersecurity Officer* in § 101.615 to clarify that the owner or operator must designate a CySO, but

they also may designate an alternate CySO to assist in the duties and responsibilities at all times, including at times when the CySO may be away from the U.S.-flagged vessel, facility, or OCS facility.

One commenter supports including the phrase ''or equivalent job experience'' to the CySO requirements.

The Coast Guard agrees that the ''or equivalent job experience'' is an important phrase and maintains it as part of the final rule in § 101.625(e).

Some commenters requested that we rename the CySO position from ''CySO'' to ''Facility Cybersecurity Officer'' due to potential confusion with other positions and titles, such as the Chief Information Security Officer (CISO) or other ''C-Suite'' personnel. These commenters expressed concern that the Coast Guard was introducing a term that has not previously been used by other agencies and offered alternative titles for the role.

This final rule clearly defines the CySO position and differentiates it from other positions and titles at a U.S.-flagged vessel, facility, OCS facility, or organization. We do not agree with changing the name of the position in this final rule, especially as this applies specifically to U.S.-flagged vessels, facilities, and OCS facilities. We selected this term to differentiate from other roles identified in existing regulations, while clearly outlining the requirements of the position. If an owner or operator prefers to refer to the position by a different title within the organization, then they are free to do so as long as they explain the different title in their Cybersecurity Plan.

One commenter expressed concern that this final rule does not address how the CySO is expected to interact with the CSO, and that the relationship between these two positions should be clearly defined. They stated that the CSO should have ultimate responsibility on all security-related matters, including cybersecurity, and that the CSO should approve the Cybersecurity Plan.

The Coast Guard notes that the roles and responsibilities of the CSO are clearly outlined in existing regulations, and the roles and responsibilities of the CySO are clearly outlined in this final rule. Any interaction between the CySO and other security positions should be determined by the owner or operator at the U.S.-flagged vessel, facility, OCS facility, or organizational level, as appropriate. As long as statutory and regulatory requirements are met, it is the discretion of each owner or operator of U.S.-flagged vessel, facility, or OCS facility to determine how their employees interact.

One commenter requested that specific criteria be developed for the CySO position to develop training programs. The commenter requested that Government-funded training courses be considered for existing CSOs to be trained for the CySO designation. This commenter also requested that third-party training programs be eligible for Federal grant programs, such as FEMA's Port Security Grant Program.

The Coast Guard notes that the criteria in § 101.625 is sufficient as baseline requirements for the CySO position. When determining the baseline requirements for the CySO, we looked at similar jobs and pulled those requirements that suited the need. The Coast Guard does not currently have plans to develop and fund training programs for the CySO position. We advise affected entities that they are welcome to work with FEMA, local port partners, their Area Maritime Security Committee, and others, as appropriate, in requesting support through any Federal grant program in support of maritime security. The decision on what is eligible for, and would receive such grant funding, is not made by the Coast Guard.

One commenter requested clarification on the specifics of cybersecurity inspections that are the responsibility of the CySO, including how they will be conducted.

Coast Guard inspections are intended to verify compliance with an approved Cybersecurity Plan. When arranging for and during the inspection, it is the responsibility of the CySO to ensure that any disruptions to operations are minimized. The cybersecurity portion of the inspection will follow standard inspections procedures, similar in methodology to physical facility inspections, in verifying compliance with the regulations. The Coast Guard may consider future policy development, if needed, on the conduct of cybersecurity inspections.

One commenter recommended mandatory training and certification for the position of the CySO. For vessel CySOs, one commenter suggested implementing a certificate of proficiency similar to those required for other roles under the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers.

After reviewing the requirements for designating a CySO, the Coast Guard is not including additional requirements or certifications at this time. This final rule provides minimum baseline requirements necessary for the identification of this role, and the Coast Guard does not intend to place too prescriptive requirements that could impede stakeholders' ability to identify suitable candidates. Owners and operators are welcome to add additional requirements on their own, so long as they meet compliance with these regulations.

Some commenters questioned why there are physical security controls under the CySO when these are under the existing purview of VSOs, FSOs, and OCS FSOs.

The Coast Guard notes that physical security controls for IT and OT systems are listed in § 101.630(c)(8) as being part of the Cybersecurity Plan, which is developed and implemented by the CySO. These regulations do not preclude the VSO, FSO, or OCS FSO from performing their required roles and responsibilities and helping to inform the Cybersecurity Plan, or otherwise working with the CySO in the completion of security-related requirements.

One commenter expressed concern that the roles and responsibilities of the CySO are too complex for just one person, and often these functions are performed by a team or multiple employees.

The Coast Guard notes that the CySO is required to ''ensure'' that certain actions are conducted and allows for them to work with the team and others who assist in carrying out those functions. The CySO is also able to assign security duties as needed.

One commenter stated that the requirements under §§ 101.625(d)(8) and 101.625(d)(9) were very similar and could be combined. The requirements in question are to ensure the cybersecurity awareness and vigilance of personnel through briefings, drills, exercises, and training and to ensure adequate cybersecurity training of personnel.

The Coast Guard agrees with this comment and removed ''through briefings, drills, exercises, and training'' from § 101.625(d)(8) to provide CySOs with more flexibility, and less prescriptive measures, on how they would meet the requirements, and also alleviate redundancy in the language between paragraphs (d)(8) and (d)(9).

Several commenters requested that the Coast Guard remove the requirement for cybersecurity inspections to be arranged in conjunction with U.S.-flagged vessel, facility, and OCS facility inspections, as a U.S.-flagged vessel, facility, or OCS facility might feel that they need to conduct the cybersecurity inspection separately due to factors such as availability of the CySO.

In this final rule, the Coast Guard revised § 101.625(d)(6), which requires the CySO to arrange for the cybersecurity inspection to reflect that cybersecurity inspections may be held in conjunction with physical security inspections, to increase flexibility and decrease burden, for the U.S.-flagged vessel, facility, or OCS facility. The Coast Guard notes that scheduling inspections is ultimately up to the local COTP or the Officer in Charge, Marine Inspections (OCMI) in working with the regulated U.S.-flagged vessel, facility, or OCS facility.

F. Comments Related to the Cybersecurity Plan

Several commenters noted that there is a lack of clarity whether one Cybersecurity Plan for a fleet is acceptable, or if each vessel and facility requires its own Plan.

Each regulated U.S.-flagged vessel, facility, and OCS facility is required to develop and maintain a Cybersecurity Plan.

Multiple commenters noted a lack of reference to ASPs. One commenter also recommended that the Coast Guard allow the Passenger Vessel Association (PVA) specific ASP. As noted in § 101.660 of this final rule, the Coast Guard will allow owners and operators to use ASPs to comply with this final rule. We added additional text to § 101.660 to clarify that ASP provisions apply to cybersecurity compliance documentation. Given the unique nature of cybersecurity threats, vulnerabilities, and mitigation strategies, owners and operators must ensure that use of ASPs includes those items specific to each U.S.-flagged vessel, facility, and OCS facility. The Coast Guard will evaluate each ASP's cybersecurity component to ensure full regulatory compliance with each applicable requirement, including the PVA-specific ASP.

One commenter recommended that § 101.630(a) be amended to add ASPs and OCS FSPs to the requirement for CySOs.

The Coast Guard partially concurs with the recommendation and added references to OCS FSPs in § 101.630(a) to clarify that OCS FSPs follow the same requirements as VSPs and FSPs. However, we do not find it necessary to add the term ''Alternative Security Program'' because ASPs are already included as an option in § 101.660 and are also expressly addressed in 33 CFR parts 104, 105, and 106.

Some commenters stated that the Cybersecurity Plan should include additional security measures for the vessel, facility, or OCS facility to take in cases of increased MARSEC levels. For instance, MARSEC Level 3 Cybersecurity Controls may involve reviewing and authorizing all remote access sessions; removing unpatched systems from direct internet access; isolating or shutting down nonessential systems; requiring multifactor authentication for all accounts; and reporting suspicious activity to stakeholders, ISACs, CISA, and the Coast Guard. Cybersecurity MARSEC actions should be specific, achievable, and deliver meaningful security benefits. This enables the vessel or facility to reduce vulnerabilities and enhance resilience, even for short periods. They also suggested that the Cybersecurity Plan should encourage owners or operators to implement additional measures anytime credible threat information is known.

This final rule does not prevent a U.S.-flagged vessel, facility, or OCS facility from adding such language or additional measures to their Cybersecurity Plan, should they desire. However, the Coast Guard did not add requirements for increased MARSEC levels in this final rule and will not mandate this language because of multiple factors. First, it is difficult to set MARSEC conditions solely based on cybersecurity threats. Cybersecurity threats are constantly evolving, with new vulnerabilities, attack vectors, and tactics emerging regularly. This makes it challenging to establish static threat conditions that can effectively address all potential scenarios. Additionally, cybersecurity threats can originate from various sources, including nation-states, cybercriminals, insiders, hacktivists, and others. Each source has different capabilities, motivations, and methods, requiring tailored threat conditions that are difficult to generalize. Even if we were to set MARSEC conditions based on cybersecurity threats, it would be challenging to list one-size-fits-all requirements that would work for a wide array of vessels and port facilities, each with different risk profiles and operational conditions. For example, vessels may face different types of cyber-attacks depending on their routes, locations, cargoes, and onboard technologies. Imposing blanket cybersecurity requirements based on MARSEC conditions may not be practical in these cases.

Furthermore, creating specific requirements for each MARSEC level would necessitate constant updates and adjustments to keep pace with the dynamic nature of cyber threats. This would place a significant administrative burden on both the Coast Guard and the maritime industry. Instead, we are maintaining a flexible and adaptive approach to cybersecurity in this final rule that allows for tailored responses based on the unique circumstances of each U.S.-flagged vessel, facility, and OCS facility.

One commenter inquired about how a CySO would respond to elevations in MARSEC levels.

The regulations in this final rule do not tie these minimum baseline requirements to elevation in enforcement due to MARSEC level. Guidance on responding to elevated MARSEC levels would come in a separate Coast Guard directive.

One commenter questioned the use of ''major amendment'' when requiring a resubmission of a Cybersecurity Plan in the regulations and suggested further clarification or definition would be needed. Another commenter expressed appreciation for the flexibility for each owner or operator to determine what constitutes a ''major amendment'' as appropriate for their organization based on types of changes to their security measures and operational risks,'' but cautioned that this creates its own uncertainty. The commenter requested that in the final rule, the Coast Guard be more explicit or provide thresholds or examples of what it considers ''major.'' The commenter also suggested that factors such as cost and operational burden should be considered (for example, more operators and employees or more equipment), and that the threshold may be a percent of the current budget for cybersecurity since each company will be different. The commenter reasoned that this threshold would also provide clarity for Coast Guard personnel. Another commenter suggested that such further clarification would be similar to the Coast Guard's clarification of ''major conversion'' for materiel requirements. Similarly, a commenter stated that the proposed 30-day notice to the Coast Guard for approval of any proposed major amendments to the Cybersecurity Plan would be overly burdensome and would likely cause the Cybersecurity Plan to be in a constant state of flux because of waiting for approvals and revisions, or could unnecessarily delay security enhancements that may trigger a required audit or approval cycle.

The Coast Guard recognizes these concerns. The Coast Guard considered the suggestion to define ''major amendment'' much like the Coast Guard has done with ''major conversion'' for materiel requirements but does not agree with it. Rather than define the term ''major amendment,'' we removed it from §§ 101.625(d)(13) and 101.630(e)(2) in this final rule. This removes any ambiguity about which

amendments require resubmission of the Cybersecurity Plan. It is also consistent with our physical security requirements in 33 CFR parts 104, 105, and 106, which do not specify that only ''major'' amendments must be sent to the Coast Guard for approval. *See* 33 CFR 104.415(a)(2), 105.415(a)(2), 106.415(a)(2). Removing the term ''major'' allows stakeholders to address amendments uniformly across both physical security and cybersecurity requirements. We retained the requirement to submit proposed amendments within 30 days but note that § 101.630(e)(2)(i) provides that nothing in this section should be construed as limiting the owner or operator of the U.S.-flagged vessel, facility, or OCS facility from the timely implementation of such additional security measures not enumerated in the approved VSP, FSP, or OCS FSP as necessary to address exigent security situations.

Some commenters recommended that the Coast Guard strike the requirements, or make modifications to the requirements, related to an owner or operator's submission of proposed amendments to the Cybersecurity Plan. Some commenters suggested tailoring this to ''material'' or ''significant'' changes.

In this final rule, the Coast Guard did not remove this requirement, as it is consistent with existing practice and 33 CFR parts 104, 105, and 106. However, we revised § 101.630 to remove ambiguity by eliminating the term ''major amendment,'' as well as the associated requirement that changes to the Cybersecurity Plan must be proposed to the Coast Guard before implementation, as discussed above. We added language to § 101.630(e)(2)(i) to address situations when an owner or operator may feel that security measures are needed while an amendment is under review by the Coast Guard.

One commenter stated that it was not clear to the owner, operator, or CySO whether they submit their Cybersecurity Plan to the COTP or OCMI, or to the U.S. Coast Guard's MSC.

Under § 101.625(d)(13), and according to § 101.630(d), the CySO must ensure the owner or operator submits the Cybersecurity Plan for approval to the cognizant COTP or OCMI for facilities or OCS facilities, or to the MSC for U.S.-flagged vessels.

One commenter suggested removing the requirement that the CySO include ''a letter certifying that the plan meets the requirements of this subpart must accompany the submission'' under § 101.630(d).

The Coast Guard agrees with this recommendation, as submitting the Cybersecurity Plan itself qualifies as certification that the Plan meets all the requirements. The Coast Guard revised § 101.630(d) to remove the requirement to send this letter.

One commenter requested clarification on whether the Cybersecurity Assessment and Cybersecurity Plan could be done separately from the existing requirements for conducting an Assessment and Plan according to 33 CFR parts 104, 105, and 106. Additionally, they sought clarification on how this final rule affects § 105.305(c)(1)(iv) for existing security measures and procedures relating to services and utilities, and § 105.305(d)(2)(v) for radio and telecommunication systems, including computer systems and networks.

This final rule allows for regulated U.S.-flagged vessels, facilities, and OCS facilities to choose whether to incorporate Cybersecurity Assessments and Cybersecurity Plans into their existing assessments and plan submissions, or to submit them as separate documents. Nothing in this final rule is meant to replace existing regulations, and regulated entities should ensure compliance with all applicable regulations. In the event there is overlap, entities may identify where requirements are being simultaneously satisfied. We revised the definition in § 101.615 of *Cybersecurity Plan* and the reference to Plan submission in § 101.630(a) to clarify that separate submissions are acceptable.

Several commenters recommended adopting various specific standards, such as the NIST CSF, NIST's special publications, the Defense Counterintelligence and Security Agency's National Industrial Security Program, DoD's Cybersecurity Maturity Model Certification program 2.0, IEc 62443, IMO, ISO/IEc 17020, the International Association of Ports and Harbors' Cybersecurity Guidelines for Ports and Port Authorities, the International Association of Classification Societies' (IACS) Unified Requirements (UR) E26 and E27, the North American Electric Reliability Corporation's CIP–013, and the American Bureau of Shipping's (ABS) Cyber Resilience Program for vessels. Other commenters inquired about leveraging third-party inspection standards, such as ISO/IEc 17020. One commenter stated that this final rule's minimum cybersecurity requirements and the ABS' Cyber Resilience Program for vessels both leverage the NIST CSF and IEc 62443 and appear to be directing the same efforts under the same framework. They inquired about ABS and Coast Guard collaboration and alignment on these efforts.

The Coast Guard intentionally created this final rule to allow flexibility in implementing a CSF. In developing this final rule, the Coast Guard leveraged CISA's Cyber Performance Goals, which themselves are mapped to NIST's CSF, but this does not preclude owners and operators of U.S.-flagged vessels, facilities, and OCS facilities from using other resources. Owners and operators may use NIST's standards or other standards and frameworks to help inform how they comply with the mandatory requirements in this final rule. This final rule provides minimum baseline requirements, but we encourage affected entities to include items in their Cybersecurity Plan that they deem in their best interest to enhance cybersecurity. Each Plan will be evaluated by the cognizant COTP or the OCMI for facilities and OCS facilities, and the MSC for U.S.-flagged vessels to ensure it meets the Coast Guard requirements.

The Coast Guard acknowledges that there are many third party and international standards and frameworks that could be used to meet the regulations. The owner or operator may use ABS or other third-party frameworks to assist them in meeting the Coast Guard's requirements, though this approach does not guarantee automatic acceptance or approval by the Coast Guard. However, the Coast Guard retains all statutory functions under MTSA and international responsibilities under the International Ship and Port Facility Security Code. At this time, we do not intend to delegate any functions to third parties under this final rule.

One commenter stated that the current format, which closely follows the regulatory format of 33 CFR parts 104, 105, and 106, was not well-suited for cybersecurity requirements, and that something more in line with NIST's Framework would be better.

The Coast Guard has chosen to articulate the cybersecurity requirements within 33 CFR part 101 because these regulations impact U.S.-flagged vessels, facilities, and OCS facilities collectively. This format is presented in a more organized and accessible manner to the maritime partners who are familiar with the MTSA regulations. Additionally, § 101.650 lists cybersecurity measures that are based on CISA's CPGs, which are aligned with NIST's CSF. This approach ensures clarity and facilitates easier compliance, allowing stakeholders to view all pertinent

cybersecurity regulations in a single, consolidated section.

One commenter felt that certain areas of the NPRM were too prescriptive, and that the Coast Guard should take an outcome-based approach of the appropriate NIST CSF function.

Pursuing an outcome-based approach was not feasible based on necessary timelines to develop and implement cybersecurity measures, and the Coast Guard feels that its rules strike the best balance of prescriptiveness because they are based on existing MTSA regulations and existing interagency guidelines generally accepted by industry. We recognize that some stakeholders may feel the requirements are too prescriptive, while others commented that the requirements were not prescriptive enough. The cybersecurity measures listed in § 101.650 are based on CISA's CPGs, which are performance-based goals and recommended actions and align with the NIST CSF. This approach ensures clarity and facilitates easier compliance, allowing stakeholders to view all pertinent cybersecurity regulations in a single, consolidated section. The Coast Guard acknowledges that there are many third-party and international standards and frameworks that could be used to meet the regulations. Owners and operators of U.S.-flagged vessels, facilities, and OCS facilities may base their Cybersecurity Plan on a standard or framework that they prefer and explain how the requirements of this final rule are met.

One commenter requested that the Coast Guard update language in the regulations to clarify that the CySO does not conduct audits but is limited to ensuring audits are conducted. Another commenter asked for clarification on the scope of the audit the CySO must perform.

The Coast Guard agrees with this suggestion and revised § 101.630(f)(2) in this final rule to clarify that the CySO does not conduct the audit themselves and that the CySO must only ensure that an audit is conducted. The Coast Guard did not add the additional language to the regulatory text defining the term audit as it allows for flexibility in how the regulated entity conducts their audit. The regulatory text in § 101.630(f) is in line with existing audit requirements in 33 CFR parts 104, 105, and 106.

One commenter expressed support for Cybersecurity Assessments being part of the Cybersecurity Plan renewal every 5 years when there is a change in vessel or facility ownership, or there are major amendments to the Cybersecurity Plan. However, they disagreed with requiring a Cybersecurity Assessment annually, citing that annual Cybersecurity Assessments are excessive for small businesses.

The Coast Guard did not make changes to the frequency required for Cybersecurity Assessments. We believe that annual Cybersecurity Assessments are important for regulated entities to continually monitor for cybersecurity developments pursuant to § 101.650(e). The cybersecurity environment can change so rapidly that conducting a Cybersecurity Assessment less frequently than annually could lead to vulnerabilities going unnoticed, with potentially drastic consequences. Moreover, the NIST guidelines state that risk assessments such as this should be conducted no less than annually. We expect that entities with a smaller or less complex IT and OT footprint will have shorter Cybersecurity Assessments with annual assessments.

G. Comments Related to Drills and Exercises

We received many comments about requirements for drills and exercises. Several commenters asked about the frequency and scope of drills and exercises. Some commenters from regulated entities noted that quarterly drills and annual exercises seemed excessive for smaller, seasonal operators and low-risk MTSA-regulated entities. These commenters suggested that quarterly drills and annual exercises would create an excessive time and resource burden on those entities, especially those with limited cyber exposure. One commenter noted that the biggest security threats facing a domestic passenger vessel remain a physical breach of security and suspicious individuals or activities associated with criminal activity and not cyber activities.

Other commenters referenced existing drills and exercise requirements for MTSA-regulated entities and recommended that the Coast Guard allow for overlap with new cybersecurity drills and exercises and existing required drills and exercises. Commenters also suggested that drills should be conducted at the organizational level rather than at the vessel or facility level. One commenter asked if drills are expected to be a comprehensive test of the Cybersecurity Plan, meaning the entirety of cybersecurity capabilities outlined in the Cybersecurity Plan. Another commenter expressed confusion regarding exercise requirements and tabletop simulation. One commenter stated that separate drill requirements were excessive and unnecessary.

Another commenter requested further explanation on required crew involvement. The commenter explained that onboard personnel have little to no involvement in cyber-specific drills and recommended the Coast Guard provide further explanation on the intent and extent of crew involvement with these drills.

The Coast Guard believes that, while different stakeholders have varying IT and OT footprints, it remains critical to incorporate some level of drills and exercises to ensure that owners, operators, and regulated entities are prepared to prevent and respond to increasing cybersecurity threats. After considering these comments, in this final rule, we have adjusted the frequency of conducting drills from quarterly to twice each calendar year. We believe that two drills annually will ensure sufficient proficiency with the procedures, while allowing for a regulated entity to conduct additional drills if they choose to, and we understand how quarterly drills and exercises could be too frequent for some vessel operations, as noted by some commenters. The Coast Guard felt that one drill annually would not be sufficient, while requiring three drills annually would not be a significant decrease from the original requirement of four drills annually. We also clarified that cybersecurity drills required under this part may be performed in conjunction with existing MTSA-required drills and exercises. We decided to maintain annual exercises but will also similarly allow exercises to be performed in combination with existing MTSA-required exercises.

While owners and operators are authorized to conduct drills at the organization level, each vessel, facility, and OCS facility has unique risks and operators at the vessel, facility, and OCS facility level should be experienced in addressing those unique vulnerabilities and prepared to respond to such incidents appropriately. This final rule states that drills should test individual elements of the Cybersecurity Plan and, therefore, are not a comprehensive test of the entirety of cybersecurity capabilities. The Coast Guard feels that tabletop exercises, if selected by the regulated entity to comply with our requirements, can serve as a full test of the CSF. This is similar to tabletop exercises under §§ 104.230(c)(2)(ii), 105.220(c)(2)(ii), and 106.225(c)(2)(ii), as participants can discuss and simulate the implementation of specific measures found within the Cybersecurity Plan.

The Coast Guard believes that this final rule provides the necessary level of detail on the requirements on the

conduct and elements of drills and exercises. This final rule allows each regulated entity the flexibility to determine the specific drills and exercises they wish to conduct. Additionally, individual stakeholders can determine the level of crew involvement in drills and exercises based on individual crew and employee roles and responsibilities within the organization.

Furthermore, the Coast Guard understands that each U.S.-flagged vessel, facility, and OCS facility operates facing different cybersecurity risks. Owners and operators may seek an exemption or waiver using the procedures in § 101.665. This flexibility is intended to accommodate varying levels of risk and operational needs across different U.S.-flagged vessels, facilities, and OCS facilities.

H. Comments Related to Records and Documentation

One commenter noted that the 2-year recordkeeping mandate could be quite costly compared to its value proposition.

The 2-year recordkeeping requirement is consistent with the existing regulations and aligns with incorporating the Cybersecurity Plan into a VSP, FSP, or OCS FSP if a regulated entity chooses to include the Cybersecurity Plan as part of their VSP, FSP, or OCS FSP. The Coast Guard recognizes that there may be varied costs associated with record keeping but expects that these additional records would be maintained similar to the existing records and could prove important in the event of a future cyber incident.

One commenter requested clarification on what the Coast Guard was not obtaining from covered entities' use of the Cyber Annex—which supports an FSP and OCS FSP—under the MCAAG.

The Cyber Annex was intended to provide only initial cyber guidance based on the regulations available at the time. Moreover, the MCAAG is only a voluntary ''how-to'' guide and is not, itself, a regulation. The Coast Guard recognizes that further actions are needed to better secure the MTS from cyber threats and vulnerabilities. This final rule is the next step for a new suite of baseline requirements specific to cybersecurity that go beyond what was addressed previously in the regulations and earlier guidance documents.

Some commenters expressed concerns over omitting FSP and OCS FSP Cyber Annexes in the new regulatory framework and the implications for companies that have already invested resources in developing these annexes.

The existing requirement for the owners and operators of MTSA-regulated facilities and OCS facilities to analyze vulnerabilities associated with radio and telecommunication equipment, including computer systems and networks, allows an owner or operator to demonstrate compliance in a variety of formats. The information may be provided in a separate Cyber Annex to the FSP or OCS FSP, or incorporated into the FSP or OCS FSP together with the physical security measures. Regulated entities who chose to create a separate Cyber Annex may use the content of the existing Cyber Annex to help develop a Cybersecurity Plan that reflects all cybersecurity measures required in subpart F, as appropriate, to mitigate risks identified during the Cybersecurity Assessment. As noted in § 101.630(a), the Cybersecurity Plan may be included in an existing VSP or FSP or VSP or FSP annex. This final rule amended § 101.630(a) to clarify that the Cybersecurity Plan may also be included in an OCS FSP, part of an approved ASP, annex to the OCS FSP, or may be provided in a separate submission (but is still considered a part of the VSP, FSP, or OCS FSP).

The Coast Guard believes that this final rule provides sufficient information for regulated entities to comply with requirements for a Cyber Incident Response Plan. The term is defined in § 101.615, and the requirements for inclusion are described in §§ 101.620(b)(6), 101.625(d)(4), and 101.650(g)(2).

One commenter noted that some ship OT systems have cybersecurity requirements as mandated by the DoD and noted that some required compliance elements pose a documentation duplication effort. They asked what exceptions would be considered for those having to meet DoD requirements.

The Coast Guard recognizes that cybersecurity requirements of other Federal agencies may be similar to these requirements. However, due to the specific nature of maritime cybersecurity considerations while operating in the MTS, the Coast Guard requires documentation specifically showing compliance with these regulations. At this time, we are not considering blanket compliance exemptions for regulations of other Federal agencies. Owners or operators may use this similar, but separate, compliance to inform their compliance with Coast Guard regulations.

I. Comments Related to Communications

One commenter noted that it was important to foster open communication and explore diverse solutions for information sharing and collaboration across stakeholders.

The Coast Guard agrees and encourages interested stakeholders to communicate and explore information-sharing solutions. These regulations are intended to establish certain baseline requirements that establish a common regulatory framework for all stakeholders to have those discussions.

J. Comments Related to Incident Reporting

The Coast Guard received numerous comments in response to our request for input on the reporting of cybersecurity incidents and whether those reports should be made to the Coast Guard through the NRC or to CISA. Commenters were split between the two options, with some citing the existing requirement to report security incidents to the NRC as a reason to maintain this process, while others cited the proposed requirements of CISA's CIRCIA rulemaking project. One commenter suggested that reporting to CISA be updated to a 72-hour requirement, whereas other comments suggested that the reporting be delayed until a cybersecurity incident has been investigated by an entity. Another commenter suggested that Global Positioning System (GPS) jamming and spoofing should be included as incidents that require mandatory reporting. One commenter suggested reporting to the Defense Cyber Crimes Center (DC3)/DoD-Defense Industrial Base Collaborative Information Sharing Environment (DCISE). One commenter suggested that reporting should not be directed to the NRC due to the NRC being short-staffed and not suited to receive the incident reports. One commenter noted that CISA is already in a position to catalog such reports and share critical information with those impacted in both private industry and Government sectors, as this is part of their current mission.

One commenter cited the various reporting requirements of CIRCIA's proposed rulemaking,[55] the Coast Guard's NPRM, Executive Order 14116 (Amending Regulations Relating to the Safeguarding of Vessels, Harbors, and Waterfront Facilities of the United States), along with the Coast Guard's NVIC 02–24 and Policy Letter 08–16. The commenter requested that the Coast

[55] 89 FR 23644, April 4, 2024.

Guard work with CISA, who is less familiar with the maritime industry, and deconflict the reporting requirements. In response to whether the Coast Guard should require reporting of ransomware payments, one commenter stated that they did not feel this would be wise. Other commenters stated that they felt that ransomware and related payments should indeed be reported. One commenter expressed concern with reporting of incidents or KEVs between CySOs, noting that information specific to a company should not be shared with other companies.

One commenter asked how the Coast Guard intended to share reported information with all regulated entities. Another commenter similarly suggested that the Coast Guard establish procedures within these regulations for the reporting of Government incidents to other parties. One commenter expressed concern that NRC personnel who will take reports of cybersecurity incidents might not be specialized in cybersecurity or have the appropriate knowledge and experience; therefore, NRC personnel would be unequipped to take reports of cybersecurity incidents. One commenter expressed concern about the limitations for vessels when reporting an incident to the NRC via telephone. The commenter noted that vessels might have limited internet connections and requested that the Coast Guard allow alternative communication methods such as very high frequency (VHF) or International Maritime Satellite (INMARSAT) as options for reporting to the NRC.

With this final rule, the Coast Guard is expecting reportable cyber incidents be reported to the NRC only by those entities not already required to report cyber incidents under 33 CFR 6.16–1, as amended by Executive Order 14116. Title 33 of the CFR, part 6.16–1, requires the reporting of evidence of sabotage, subversive activity, or an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility, which includes all current MTSA-regulated U.S. vessels and facilities regulated by this rule. 33 CFR part 6.16–1 does not apply to OCS facilities regulated under 33 CFR part 106. Therefore, those OCS facilities are subject to the reporting requirements of this rule. Reporting to the NRC by these entities is in line with established requirements and timelines, including under § 101.305. It also enables a timely response to incidents by the Coast Guard, as well as partner agencies with whom the NRC shares incident reports immediately upon receipt. To minimize duplicative reporting from the same entity, the requirement to report under this final rule does not apply if the entity has reported the cybersecurity incident to the Coast Guard pursuant to 33 CFR 6.16–1, highlighting that because OCS facilities are not subject to the reporting requirements in 33 CFR part 6, OCS facilities must report cyber incidents to the NRC under this final rule.

Entities subject to reporting cybersecurity incidents under 33 CFR 6.16–1 must also report to the FBI and CISA, and they may also be subject to reporting to CISA under CIRCIA once the final rule is published and effective. The Coast Guard and CISA are committed to minimizing the burden on entities and will assess the need for additional policy guidance regarding the content of reports and the mechanism for reporting to satisfy applicable requirements in this part, § 101.305, 33 CFR part 6, and the CIRCIA final rule to be issued by CISA. The Coast Guard and CISA are committed to proactively collaborating and issuing guidance to entities to harmonize cyber reporting requirements to the extent possible and to clarify procedures for reporting cyber incidents to the Coast Guard and to CISA, respectively under current regulations, as well as in the future once CIRCIA's regulations take effect.

Cyber incident reports to the Coast Guard and CISA serve complementary but distinct operational purposes that are consistent with each agency's respective missions and authorities. Reports to the Coast Guard ''without delay'' under this part, § 101.305, and 33 CFR part 6 serve as an immediate notification to support the rapid response to events that may result in a TSI. Notifications to the NRC are immediately shared with CISA, FBI, and other relevant agencies to allow for the earliest mobilization of response and resources. Cyber incidents can quickly escalate and evolve, and any delays to the reporting can affect the ability to successfully respond to an incident. Reporting to the NRC without delay allows the Coast Guard COTPs to understand the potential risks of an incident and apply their authority to protect the MTS, including the use control and compliance measures as provided at § 101.410. In many cases, the goal of the initial response is to ensure public safety, mitigate the consequences of disastrous events, or prevent cascading impacts on critical infrastructure or the public. This includes but is not limited to minimizing loss of life and property, preventing environmental disasters or other accidents at sea, assisting in the recovery of critical IT or OT systems at ports or other facilities, defending the sovereignty of the United States, and facilitating legitimate use of maritime waterways. After the initial response, the notifications enable the Coast Guard to evaluate the broader risks to the MTS based on the specific vulnerability.

Separate from the Coast Guard's authorities under MTSA, but consistent with what Congress has envisioned in CIRCIA, reporting ''covered cyber incidents'' to CISA under its future regulation within 72 hours of having a reasonable belief that such an incident occurred (and ransom payments resulting from a ransomware attack within 24 hours of the payment being made) serves a complementary but distinct operational purpose from Coast Guard reporting requirements. As the lead agency for Federal cybersecurity and the national coordinator for critical infrastructure risk and resilience, CISA is well-positioned to support Coast Guard cyber related operations and address cross-sector cyber risk more broadly under its forthcoming CIRCIA regulations. By collecting more technical information via the CISA incident report then was collected by the NRC in the initial report and cross-referencing that information with other incidents reported in other critical infrastructure sectors, CISA can support the Coast Guard's operations, assist other entities in the MTS in mitigating exploited vulnerabilities, quickly identify other entities that may be at risk across critical infrastructure sectors, automate sharing information across the public and private sectors to protect against similar incidents in the future, and counter sophisticated cyber campaigns earlier.

CISA's further sharing of reported threat activity and impact information (for example, techniques, tactics, and procedures used to cause physical, functional, or informational impacts) will enable other Federal and non-Federal stakeholders to more effectively allocate resources and inform the development of more secure products. Furthermore, reporting incidents to CISA under the CIRCIA final rule will improve the U.S. Government's collective visibility into the national cyber threat landscape and close critical information gaps.

The Coast Guard does not specify specific incident types in this final rule but relies on the definition of reportable cyber incidents, as well as existing definitions for *breaches of security* and *transportation security incidents,* as defined in § 101.105, and *suspicious activity* as described in § 101.305.

The Coast Guard through this final rule is not requiring reporting to any entity outside of the NRC, such as DC3

or DCISE, as the NRC already has an established process and relationship with the regulated entities affected by this final rule.

The Coast Guard disagrees that the NRC would be unable to accommodate reported cybersecurity incidents. The NRC already receives reports of cybersecurity incidents according to the reporting requirements of § 101.305, which includes cybersecurity.

The Coast Guard agrees that reporting requirements, including those of existing MTSA regulations, this final rule, and the recent Executive Order 14116 updating 33 CFR 6.16–1 on cybersecurity, should be harmonized to the extent practicable and in accordance with the law. Policy Letter 08–16 was superseded by NVIC 02–24, which provides guidance on existing MTSA reporting requirements as well as those addressed by the recent Executive Order. The Coast Guard will work with partner agencies to maximize harmonization and alignment with this final rule to the extent practicable by assessing the need for new policy guidance regarding reporting requirements under this final rule, 33 CFR 6.16–1, and the CIRCIA final rule to be issued to CISA.

The definition for a reportable cyber incident provides regulated entities with sufficient information to determine when to report a ransomware incident. The Coast Guard did not add a requirement for the reporting of a ransomware payment. Note that a separate requirement to report ransom payments to CISA may be included in the forthcoming CIRCIA final rule issued by CISA.

In § 101.650(e)(3)(iii), this final rule requires each owner or operator of a regulated entity to maintain a method to share threat and vulnerability information with external stakeholders, but does not require sharing information with private companies that have no relationship with the regulated entity or do not have a role in facilitating cybersecurity response or the cybersecurity posture of the regulated entity.

The requirements in this final rule for reporting cybersecurity incidents apply to U.S.-flagged vessels, facilities, and OCS facilities and detail how to report to the Government. This final rule does not establish requirements for the Government to share information with the public, and the Coast Guard does not intend to immediately share cybersecurity incident reports from a regulated entity with other private stakeholders. If needed, the Coast Guard or other agencies can develop bulletins, advisories, or other guidance to address cybersecurity threats, risks, and vulnerabilities that may be discovered. Similarly, this final rule does not establish processes or procedures for the Government to report its own incidents to the public, as this final rule only addresses requirements for those entities addressed under the Applicability section in § 101.605.

The Coast Guard disagrees with any suggestion that NRC personnel would be unable to take a report of a cybersecurity incident. NRC personnel stand watch 24 hours a day, 7 days a week, receive cybersecurity incident reports according to § 101.305, and have demonstrated the capability to collect the necessary required information made in an initial incident report. Upon receipt of the incident report, the NRC immediately shares the information with the Coast Guard Cyber Command (CGCYBER), DHS, CISA and other relevant Government agencies that have the specialization, knowledge, and experience to conduct any further follow up after the initial report.

The Coast Guard is not prescribing an alternative reporting process through VHF or INMARSAT, but this final rule does not limit the reporting of reportable cyber incidents by telephone only and affirms reports can be made by any means necessary. Vessels without connectivity are encouraged to use alternative methods to contact their designated person ashore to assist with reporting the incident without delay.

One commenter suggested that a vessel's RO be the one to report cyber issues to the Coast Guard.

The Coast Guard disagrees with this suggestion. This final rule provides sufficient clarification as to which entities should be reporting in each situation (for example, an assessment, audit, or a reportable cyber incident), and is consistent with existing MTSA regulations.

One commenter recommended that organizations develop tiered levels of cyber incident events and incidents in their Cyber Incident Response Plan.

The Coast Guard agrees that owners and operators of U.S.-flagged vessels, facilities, and OCS facilities should take the approach that best suits their needs when developing their Cyber Incident Response Plan. However, the Coast Guard does not prescribe any specific requirements in this final rule. While a tiered approach to cyber incident reporting can provide structure, it may inhibit the adaptability and responsiveness that are crucial for effectively managing cyber incidents in a rapidly evolving threat landscape. The Coast Guard prefers owners and operators to customize their incident response plans to meet their unique needs and requirements.

K. Comments Related to Cybersecurity Measures (§ 101.650)

One commenter requested that § 101.650 for cybersecurity measures include a caveat that, in situations when security measures might create safety risks, then the safety concern is to be prioritized.

The Coast Guard appreciates the concern for safety, and we do not intend for these regulations to conflict with other Coast Guard regulations for safety. The Coast Guard does not foresee a degradation in physical safety caused by these cybersecurity regulations and believes it would generate confusion if an undefined safety-based caveat were included. If owners or operators have concerns with specific application of the cybersecurity regulations, the Coast Guard encourages those owners and operators to discuss with the cognizant COTP, OCMI, or MSC, as appropriate. This final rule provides procedures for requesting equivalencies or waiver from the Coast Guard, if appropriate, in § 101.665.

One commenter suggested that cybersecurity measures be incorporated for heightened threat periods.

The Coast Guard has issued these regulations as baseline cybersecurity requirements, as cybersecurity can pose a risk at all times, even under normal threat periods. The Coast Guard encourages owners or operators of U.S.-flagged vessels, facilities, and OCS facilities to address and incorporate cybersecurity measures for heightened threat periods, if desired and as best fits their needs. The Coast Guard is also able to issue cybersecurity guidance or directives as needed, if there are specific threats and incidents. At this time, we do not believe that any specific and standing requirements for heightened threat periods should be added to this final rule.

One commenter requested that the Coast Guard add language specific to GPS denial and spoofing, and Automatic Identification System (AIS) and timing concerns.

The Coast Guard is not including a definitive list of systems and equipment in this final rule. We encourage affected entities to address those vulnerabilities which they identify in their own Assessments, or are otherwise concerned about, and to tailor drills and exercises to those areas where they have the most concern, which may include GPS denial and AIS spoofing. We also do not mandate training or drills on specific vulnerabilities or threats.

One commenter asked why outdated CPGs were used for the NPRM.

At the time the Coast Guard initially developed these regulations, Version 1.0 of CISA's CPGs were the most recent. The Coast Guard conducted an analysis to identify any significant changes between versions 1.0 and 2.0 and made changes to the regulatory text where appropriate. Only minor changes were needed. The Coast Guard will continue to monitor CISA's efforts related to CPGs to determine whether a subsequent rulemaking will be needed in the future.

One commenter suggested that the Coast Guard should clarify how this final rule applies to facilities already regulated by other authorities, particularly TSA's Security Directives. The commenter also suggested that docking ship connections be limited to systems essential for mooring, emergency operations, and ship-to-shore communications.

If an owner or operator is concerned that it may be subject to TSA's requirements and needs clarification on harmonizing compliance between TSA and Coast Guard requirements, they should notify the cognizant COTP or OCMI. If appropriate, the Coast Guard will consider procedures for waivers or equivalents in § 101.665 or have additional conversations with TSA. The Coast Guard is not placing specific requirements on what docking ship connections are allowed, and instead leaves this determination to the owner or operator.

One commenter recommended inclusion of additional requirements for logs, as well as a Shipboard Security Information and Event Management. They further recommended requirements for post-shipyard inspections and maintenance, particularly after a vessel departs an adversarial port.

The Coast Guard seeks to strike a balance and chose not to impose requirements that would be so prescriptive that compliance would be too difficult for some segments of the regulated industry. These requirements generally provide latitude for owners, operators, or CySOs to determine the specific means needed to comply with the regulatory requirements. These regulations represent minimum baseline requirements, but the Coast Guard encourages regulated entities to take any additional actions they feel are necessary to address their cybersecurity needs, so long as such additional cybersecurity measures are documented in their Cybersecurity Plans.

L. Comments Related to Account Security Measures (§ 101.650(a))

Some commenters requested changes to the section on account security measures, seeking to modify requirements for account lockout, multifactor authentication, and user credentials as they relate to certain OT systems. They expressed concerns that these measures could disrupt critical operations, deny access during emergency situations, and potentially be exploited by malicious actors to halt operations. One commenter suggested an outcome-based requirement for OT systems because the prescriptive approach may not suit many organizations and could quickly become outdated due to advancing technology.

The Coast Guard reviewed § 101.650(a) and revised specific requirements as appropriate, as they relate to OT systems. In some cases, we maintained the proposed text in line with CISA's CPGs, recognizing what provided the best level of cyber protection. The Coast Guard recognizes that OT systems may have unique considerations that are different from IT systems. The Coast Guard agrees that automatic account lockout in OT systems could have catastrophic consequences in emergency situations. We adjusted these requirements to reflect updates that CISA provided to its CPGs based on public comments they received. These updated requirements took into consideration the concerns noted in public comments that certain items, such as account lockout and multifactor authentication when applied to OT systems, could result in the concerns noted by the public comments.[56] Based on this review, we revised § 101.650(a)(1) to remove the references to OT systems and automatic account lockout due to failed logins.

The Coast Guard disagrees that these requirements are too prescriptive. The Coast Guard reiterates that these regulations represent minimum baseline requirements, and owners and operators are welcome to take additional actions and measures as they deem necessary or appropriate to best protect their systems and equipment. In cases when owners or operators do not feel that they can comply with account security measures, or that they feel a requirement is unnecessary, they may submit a request for a waiver or equivalent using the procedures in § 101.665.

One commenter noted the benefits of zero-trust architecture. Some commenters noted the importance of logs in detecting and responding to cyber-attacks and recommended that we accept next-generation logging capabilities. One commenter offered an example of one such system.

The Coast Guard notes that zero-trust architecture is one of many solutions that organizations may choose to use to comply with this final rule. The Coast Guard does not prescribe specific systems or equipment or ways to comply with these requirements. The Coast Guard recognizes that there are multiple systems, equipment, and products available, and it is up to the owner or operator to identify the option that best suits their needs while ensuring they meet the requirements of this final rule.

Some commenters expressed concern with multifactor authentication on vessels. They stated that the owner or operator should have flexibility to adequately and specifically address this, rather than a prescriptive approach. These commenters noted it is challenging especially for internationally operating vessels with a constantly changing crew and limited or no access to internet while in transit. They also stated that providing mobile phones to the crew is not advisable, noting that encouraging the use of personal devices may lead to significant resistance. The commenters believed that an alternative, such as hardware tokens for two-factor authentication, presents challenges, including distribution, configuration, and the risk of tokens being misplaced. Another commenter requested that multifactor authentication only be in place for remote access from untrusted networks into OT systems according to IACS UR E27 [57] for new ships, and with an implementation period for existing ships.

The Coast Guard recognizes that measures such as two-factor authentication may pose unique challenges to vessels, but also notes that there are multiple ways to implement multifactor authentication that do not require internet access. While carriers may not currently provide phones or other devices for this purpose, the nature of this being new rulemaking lends itself to the realization that owners and operators may have to take actions and steps that were not previously done, if that is how they determine they can best comply with the regulations. It is up the owner or operator to implement appropriate multifactor authentication given their

[56] *See https://www.cisa.gov/cybersecurity-performance-goals,* accessed November 12, 2024.

[57] IACS UR E27, Cyber Resilience of On-Board Systems and Equipment, press release information available at: *https://iacs.org.uk/news/iacs-ur-e26-and-e27-press-release,* accessed August 16, 2024.

business operations and accessibility to internet connectivity. Such multifactor authentication may include a variety of methods, including passwords, physical devices such as security tokens or access cards, or biometrics. Additionally, as is the case for all requirements in this final rule, if an owner or operator has reviewed all possible options and determines that they cannot comply with any aspect of the regulations, they may follow the process for requesting a waiver or equivalence. The Coast Guard is not relaxing the requirements further for U.S.-flagged vessels. If owners or operators do not feel that they can comply with account security measures, they may submit a request for a waiver or equivalent using the procedures in § 101.665.

One commenter requested clarification on the use of passwords; if they are required, and, if so, what the requirements for them would be.

The Coast Guard does not mandate the use of a password, only that if passwords are used or if a system is capable of password protection, the passwords are of sufficient strength and meet certain criteria to help defend against cyber-attacks based on the criticality of the system as described in § 101.650(a).

M. Comments Related to Device Security Measures (§ 101.650(b))

One commenter expressed concern about including a network map in the Cybersecurity Plan.

The Coast Guard recognizes the sensitivity of network maps. We revised § 101.650(b) to clarify that each owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must ensure the device security measures are in place, addressed in Section 6 of the Cybersecurity Plan, and made available to the Coast Guard upon request. Therefore, network maps do not need to be submitted with the Plan, but they must be maintained by the regulated entity and made available to the Coast Guard upon request.

One commenter noted that far too few entities have inventoried their IT and OT assets and supported the requirement to maintain an up-to-date asset inventory. The commenter also noted that recognizing the unique needs and limitations of OT environments is essential for effective cybersecurity regulation and implementation. Finally, the commenter strongly supported the requirement for owners and operators of covered infrastructure to designate and inventory critical IT and OT systems. The commenter noted, however, that frequent IT patches and updates are impractical in OT environments, as they can disrupt critical operations and complicate compatibility testing due to real-time demands.

The Coast Guard appreciates the support for an IT and OT system inventory. It is up to the owner or operator to determine the frequency at which OT patches and updates are conducted according to their Cybersecurity Plan to mitigate the risks identified in their Cybersecurity Assessment.

Several commenters indicated concerns regarding requirements relating to OT systems. Paragraph (e)(3)(v) of § 101.650 indicates that no OT system is to be connected to the publicly accessible internet unless explicitly required for operation, if there is documented justification. However, the commenters noted that an OT system connected to the internet can transmit machine data to the manufacturer, enabling the manufacturer to offer Smart Planned Maintenance decision support to the owner.

The Coast Guard appreciates these concerns and notes that each situation will be evaluated on its own merits on a case-by-case basis. Regulated entities may discuss specific concerns with the cognizant COTP, OCMI, or the MSC as appropriate. An owner or operator may also request a waiver or equivalence determination for the requirements according to the procedures in § 101.665.

Several commenters indicated concern regarding creating and maintaining an approved list of hardware, software, and firmware.

The Coast Guard acknowledges the potential burden in creating an approved list of hardware, software, and firmware; however, it is necessary to increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software. The Coast Guard anticipates that after developing the initial list, it will be easier for owners and operators to update the list in the future. Owners and operators may also find that their list is similar across multiple vessels or facilities within their organization. The Coast Guard does acknowledge that this will rely on coordination and cooperation of vendors and managed service providers.

One commenter requested clarification whether the proposed requirements are applicable only to mission critical IT and OT systems, or, applicable to all onboard IT and OT systems.

The Coast Guard revised this final rule to clarify where the regulations apply to all IT and OT systems and where they apply to the critical IT and OT systems. For example, we removed reference to OT systems in § 101.650(a)(1) and specified that the requirements in § 101.650(e)(1)(i) and (iv) are for critical IT and OT systems.

One commenter stated that the requirement in § 101.650(b)(2) to ensure applications running executable code must be disabled by default on critical IT and OT systems is unclear and requested adjustment to the text.

The Coast Guard disagrees that this text is unclear. The text requires entities to disable applications running executable code on critical IT and OT systems. The primary vulnerability associated with executable code is the potential for malicious code to be embedded within them, allowing attackers to exploit vulnerable systems when users open certain programs without being aware what is being done in the background. This essentially turns the device into a vehicle for launching cyberattacks or can lead to data theft, unauthorized system access, and other harmful actions. Executable code technologies include Java applets, JavaScript, HTML5, WebGL, and VBScript as well as macros used within products like Microsoft Office. IT and OT personnel will be familiar with the vulnerabilities associated with executable code and will understand the requirements of this provision.

N. Comments Related to Data Security Measures (§ 101.650(c))

One commenter stated that the phrase ''document and mitigate any vulnerabilities'' in § 101.650(e)(1)(iv) caused concern with the use of the word ''any,'' as there may not be mitigations or patches available.

The Coast Guard revised paragraph (e)(1)(iv) in § 101.650 to clarify that the regulated entity will ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems, without delay, at the time of their annual assessment, as well as part of routine maintenance.

One commenter expressed concern about the lack of specificity in the level and type of logging and monitoring of IT and OT systems for breaches of security, suspicious activity, TSIs, and cyber incidents.

Given the wide array of IT and OT systems, mandating a one-size-fits-all level of logging is not practical. Each U.S.-flagged vessel, facility, and OCS facility should customize its logging system to best address its specific risks

and technologies and document the customization in the Plan.

Some commenters expressed concern about encrypting data, at transit and at rest, on IT and OT systems, as it may be difficult to do on OT systems, or other legacy systems.

The Coast Guard revised § 101.650(c)(2) to better describe our expectations regarding data encryption. The revised text specifies that effective encryption must be deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic, when technically feasible. Encrypting data, at transit and at rest, is an example of when a requirement may not be technically feasible. In this case, the regulated entity should describe the aspects that they can comply with in their Cybersecurity Plan. Additionally, if an owner or operator has further concerns about how they can comply with these requirements, they can follow the process for requesting a waiver or equivalent according to § 101.665.

One commenter recommended that the Coast Guard add specific requirements for wireless communications as noted in IACS UR E26 4.2.5.3.[58]

The Coast Guard has not added specific requirements for wireless communications. During their Cybersecurity Assessment, each owner or operator of a regulated U.S.-flagged vessel, facility, or OCS facility may identify wireless communications as part of their IT and OT systems and equipment being assessed, as applicable.

One commenter suggested adding the requirement that remote connections to OT systems be made with secure connection and endpoint authentication, protection of integrity and authentication, and encryption at network or transport layer.

The Coast Guard disagrees that additional requirements are necessary. This final rule's requirements for remote connections are sufficient as minimum baseline requirements as noted in § 101.650(a)(4). Owners or operators of U.S.-flagged vessels, facilities, and OCS facilities are welcome to take additional measures as appropriate to their systems, equipment, and operations.

Some commenters questioned the requirements for all data requiring encryption. Another commenter suggested that data security should include PII, to include employee records and access control data, such as access control databases used for physical access, which could include information on Transportation Worker Identification Credentials, other PII, etc. Physical Access Control Systems (PACS) log physical entries into a facility, and this should likewise be treated as PII and sensitive security information. When practical, PACS servers, networks, devices, applications, and software should be air-gapped or isolated from IT and OT networks to prevent intrusion or alteration of data to allow unauthorized physical access.

The Coast Guard revised § 101.650(c)(2) to clarify that only sensitive data be encrypted. The Coast Guard has not, however, added these specific items to the requirements, but, rather, allows for the owner or operator to determine whether this is considered sensitive data subject to the requirements of this regulation.

One commenter asked if there would be specific guidance on PACS, emergency management devices or applications, OT applications and architecture, and safety devices.

The Coast Guard notes that items related to the safety and security of the U.S.-flagged vessel, facility, or OCS facility, as it pertains to cybersecurity threats and vulnerabilities to such systems, should be addressed within the Cybersecurity Plan as determined by the owner, operator, or CySO according to the requirements stated in this final rule. The Coast Guard will determine whether it is necessary to address this further in future guidance.

One commenter inquired how facilities will address PACS and emergency management systems that are network-enabled. The commenter recommended that the Coast Guard add regulatory language speaking to the interdependency of the FSO and the CySO with respect to placing, conducting maintenance, and monitoring PACS.

The Coast Guard does not agree that such regulatory mandates are needed to address interdependency of the FSO and CySO as it is up to the owner, operator, FSO, and CySO to establish relationships and ensure personnel with security duties are interacting to support the full safety and security of each U.S.-flagged vessel, facility, and OCS facility.

One commenter suggested that PACS be included in the requirement for backing up critical IT and OT systems.

The Coast Guard has determined that the CySO is best positioned to determine and should have the discretion to identify whether a system would be included under critical IT or OT systems.

One commenter questioned the requirement that the owner or operator must ensure that users maintain separate credentials on critical IT and OT systems, which could be read to mean that individual users must have different usernames and passwords for each of the critical systems to which they have access. The commenter was concerned that even if the intent is to limit shared accounts, this is not always technically feasible for OT systems.

The Coast Guard has not changed the text in § 101.650(a)(6), which requires separate credentials for IT and OT systems. The requirement sets out the measures that owners or operators must take, which are minimum baseline requirements noted in § 101.650(a). If an owner or operator does not feel that they can comply with the requirements as written, they may follow the process for requesting a waiver or equivalent according to § 101.665.

One commenter requested clarification of the Coast Guard's proposed data security measures in § 101.650(c). The commenter stated that the term ''data logs'' is undefined, makes it unclear as to what is required and whether encryption with a suitably strong algorithm is appropriate.

The Coast Guard has added a definition for the term ''logs'' to these regulations and updated the requirement in the regulation from ''data logs'' to ''logs,'' consistent with NIST and CISA's Cyber Performance Goals. In addition, we revised § 101.650(c)(2) to provide that effective encryption must be deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic, when technically feasible, rather than the proposed regulatory text requiring it be encrypted ''using a suitably strong algorithm.'' We made that change based on the feedback that the standard was unclear.

O. Comments Related to Cybersecurity Training for Personnel (§ 101.650(d))

One commenter requested clarification on how often OT-specific training should be conducted, and what topics it should cover.

Given the wide array of OT systems (for example, crane control, navigation, propulsion and steering control) and operational settings (for example, different types of vessels and port facilities), mandating a one-size-fits-all cybersecurity training is not practical. Owners and operators of each type of U.S.-flagged vessel, facility, and OCS facility will need to customize their training so that it addresses the specific risks and technologies of each regulated entity. The timeframe and frequency for

[58] IACS (UR E26 4.2.5.3) Cyber Resilience of Ships: *https://www.american-club.com/files/files/ur-e26-new-apr-2022.pdf,* accessed November 13, 2024.

completing cybersecurity training are described in § 101.650(d)(4) of this final rule.

Some commenters stated that the requirements for training are overly broad and burdensome, and difficult to track and ensure training for contractors and temporary workers. They suggested that the requirements for training be updated to ease the required training. Others noted that it would not be possible to obtain training within 5 days of gaining system access. Some suggested that the training requirements be eliminated for contractors completely.

The Coast Guard disagrees that the training is overly burdensome. The nature of cybersecurity, the growing presence of cyber systems in the operations of U.S.-flagged vessels, facilities, and OCS facilities, and the evolving nature of cybersecurity threats and vulnerabilities necessitate that personnel who will be operating within the IT and OT environment be sufficiently trained. This includes contractors, whose access to IT and OT systems and equipment may be no different than that of regular employees when it comes to potential impacts and need for training and awareness. We recognize that some contracted and part-time personnel will be on board and operating on IT and OT systems and equipment for such a short duration that meeting the training requirements may be difficult, and there may be situations where an employee may not be able to receive initial training within the timeframe stated in this final rule. To accommodate this, we revised § 101.650(d)(3) to allow for those personnel to be escorted or accompanied by personnel who already have the required training.

One commenter recommended that the Coast Guard formalize training and leverage industry best practices to apply to maritime operations.

The Coast Guard does not prescribe specific training programs or methods in this final rule. It is at the discretion of each owner or operator of a U.S.-flagged vessel, facility, or OCS facility to determine the training program that best meets their individual needs. The Coast Guard encourages maritime stakeholders to work together to share best practices.

One commenter stated that the § 101.650(d)(1)(i) requirement for training on relevant provisions of the Cybersecurity Plan was vague. They also noted that the § 101.650(d)(1)(iii) requirement for all personnel to be trained on techniques used to circumvent cybersecurity measures was a suboptimal blanket approach and should be limited in some manner. Another commenter requested that the Coast Guard clarify the specific requirements, cadence, and expectations for training programs, drills, and audits.

The training required by this final rule provides the best baseline requirements to protect IT and OT systems and equipment, as well as the personnel operating the systems and equipment. The Coast Guard believes educating relevant personnel on these techniques, they become more aware of potential risks and can recognize suspicious activities. This knowledge fosters a culture of vigilance and preparedness. However, it is up to the owner or operator, in conjunction with the CySO, to determine, which provisions of the Cybersecurity Plan apply, depending on the individual employee requiring the training. The requirements, cadence, and expectations are sufficiently addressed in these regulations, while providing regulated entities with the necessary flexibility to determine how to comply with these regulations while accounting for their unique systems, equipment, and operations. If an owner, operator, or CySO has any questions, they may bring them to their COTP, OCMI, or MSC, as appropriate.

P. Comments Related to Risks and Vulnerabilities (§ 101.650(e))

One commenter suggested that the Coast Guard use Federal Advisory Committees to develop a rank-ordered list of cybersecurity risks to be used as a benchmark against which objectives could be pursued.

The Coast Guard recognizes the benefits of working with Federal Advisory Committees but is not using a rank-ordered list of cybersecurity risks to develop the requirements. As such, there is no need to work with Federal Advisory Committees to develop such a list. Our requirements for conducting a Cybersecurity Assessment and developing a Cybersecurity Plan are designed to help each owner or operator identify the particular cybersecurity risks and vulnerabilities at the regulated U.S.-flagged vessel, facility, or OCS facility.

Some commenters suggested that the Coast Guard change the requirements for the frequency of audits, assessments, and amendments. One commenter stated that it was unnecessary to conduct these if no systems or equipment has changed.

Coast Guard does not concur with the comments. The audit and assessment intervals in § 101.630(f) are appropriate for assessing rapidly changing cybersecurity risks, vulnerabilities, and threats. Moreover, these audit and assessment intervals are consistent with existing requirements in 33 CFR parts 104, 105, and 106. The Coast Guard disagrees that no change in systems or equipment means a Cybersecurity Assessment is unnecessary because the fact that there has been no change does not mean there is a lack of new threats or vulnerabilities.

One commenter recommended that the Coast Guard change ''mitigate'' to ''manage'' when referring to responding to vulnerabilities under ''risk management'' in these regulations. The commenter also suggested that the Coast Guard change the requirements on the frequency of these actions. Another commenter suggested that patching and mitigating of vulnerabilities be done according to an organization's policies and procedures, as opposed to the requirements stated in these regulations.

The Coast Guard revised § 101.650(e)(1)(iv) to remove ''mitigate any unresolved vulnerabilities'' and, instead, require that the owner or operator ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems, without delay. The Coast Guard did not alter the frequency for the requirement, as we believe that ''without delay'' is more appropriate than ''per the organization's vulnerability management policies and processes.'' Owners and operators of U.S.-flagged vessels, facilities, and OCS facilities subject to this final rule may not have vulnerability management policies and processes that would adequately protect their critical IT and OT given the current cybersecurity risks and threats. Therefore, ''without delay'' provides the expectation to all entities subject to this final rule that identification and mitigation of all KEVs in critical IT or OT systems is necessary to prevent a cyber incident. This provision also ensures the patching and documented compensating controls take place when there is a KEV in a critical IT or OT system. An owner or operator who is unable to meet the requirements of subpart F may seek a waiver or an equivalence determination using the procedures in § 101.665.

One commenter stated that no maritime organization should ever be made to ensure that no zero days could ever exist for their internet connected systems.

The Coast Guard does not reference zero-day vulnerabilities in these regulations. In § 101.650(e)(3)(iv), we require that owners and operators of U.S.-flagged vessels, facilities, and OCS facilities must ensure there are no exploitable channels directly exposed to

internet-accessible systems. The owner or operator should take precautions based on their risk posture to ensure that all internet connections are protected and monitored appropriately when complying with these requirements.

One commenter noted that arranging for Cybersecurity Assessments in conjunction with security inspections for vessels, facilities, and OCS facilities might not be realistic. The commenter also noted that a Cybersecurity Assessment conducted at the enterprise level would be more advantageous.

The Cybersecurity Assessments, audits, and inspections are each separate actions, and may need to be separate. Audits and assessments are conducted by the regulated entity, which are separate from inspections conducted by the Coast Guard. With respect to the commenter's preference for an enterprise-level Cybersecurity Assessment, while some aspects of the Cybersecurity Plan might be similar throughout an enterprise, each regulated U.S.-flagged vessel, facility, or OCS facility possesses unique aspects and characteristics that likely pose particular risks that must be addressed on an individual basis.

Some commenters questioned the use of the term ''without delay,'' and stated that it was unclear. Its interpretation may differ by each organization, potentially ranging from minutes to hours or even days.

The term ''without delay'' is recognized in existing MTSA regulation (§ 101.305 (a)) and requires urgent action as soon as reasonably and safely possible. This term represents the criticality of the action being required. For situations in this final rule when urgency is expected because of the critical nature of the threat, the expectation is that action should be taken as soon as possible, taking into account any immediate safety concerns. The Coast Guard clarified the requirement to read ''as soon as reasonably practicable, in light of the individual circumstances, but, in any case, not longer than 96 hours'' where appropriate throughout the regulatory text in this final rule. The 96-hour limit is intended as a reasonable timeline for owners and operators to accomplish any related processing and paperwork for administrative matters that are important, but do not rise to the level of urgency as other critical security actions that must be taken ''without delay.'' In the event that a CySO, owner, or operator believes more time is necessary they may discuss their concerns with the COTP or MSC who may grant additional time if warranted.

One commenter indicated concern with the consistency of accepting mitigations for unresolved vulnerabilities and inquired whether mitigations provided by owners would generally be accepted.

Each situation will be evaluated on its own merits on a case-by-case basis. Regulated entities may discuss specific concerns with the cognizant COTP, OCMI, or the MSC, as appropriate. The Coast Guard provides procedures in § 101.665 for an owner or operator to request a waiver or equivalence determination for the requirements.

One commenter stated that the minimum requirement of patching or implementing countermeasures for all KEVs is too prescriptive and noted that OT environments, patches, and countermeasures are often unavailable. Another commenter noted that CISA already has a KEV system in place and the Coast Guard should not require another one in this rulemaking.

This final rule allows either patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems. Owners and operators are welcome to use an established process to comply with the requirements of these regulations.

Some commenters indicated concern with the proposed definition of *known exploited vulnerability (KEV)* and highlighted that the Coast Guard did not reference CISA's Known Exploited Vulnerability Catalog. The commenter also noted that the definition of *multifactor authentication* needs adjustment. Additionally, the commenter pointed out that multifactor authentication is not always technically feasible.

The Coast Guard intends its definition of *known exploited vulnerability* to be interpreted based on CISA's Known Exploited Vulnerability Catalog that CISA maintains and updates as necessary. The Coast Guard revised § 101.615 to reflect the recommended adjustment to *multifactor authentication.* With respect to concerns about the technical feasibility of multifactor authentication, the Coast Guard allows an owner or operator to request a waiver or equivalence determination using the procedures in § 101.665. Owners and operators may also discuss specific concerns with the cognizant COTP, OCMI, or the MSC, as appropriate.

Some commenters suggested the Coast Guard revise the requirements for amending Cybersecurity Plans to account for situations when an owner or operator believes they need to make an amendment and take associated action immediately because of a cyber threat, even while the cognizant COTP, OCMI, or MSC is still reviewing the Plan.

The Coast Guard revised § 101.630(e) to add a new paragraph (e)(2)(i) that states that nothing in that section should be construed as limiting the owner or operator of a U.S.-flagged vessel, facility, or OCS facility from the timely implementation of such additional security measures as necessary to address exigent security situations.

One commenter expressed concern that the 60 days for an owner or operator to amend a Cybersecurity Plan and cure deficiencies that may be identified by the COTP, OCMI, or MSC was an arbitrary number. The commenter noted that 60 days may be insufficient, as vessels operate internationally and access to materials and equipment may not be readily available and suggested a more practical timeframe of 180 days to address a deficiency.

The Coast Guard revised § 101.630(e)(1)(ii) to clarify that the owner and operator will have at least 60 days to submit its proposed amendments. We are not extending the timeframe to address a deficiency to 180 days because that period would be excessive in many cases. Many cybersecurity deficiencies need to be resolved quickly. If an owner or operator determines that more time is needed, then they should communicate the need to the COTP, OCMI, or the MSC, as appropriate.

Q. Comments Related to Penetration Testing (§ 101.650(e)(2))

Some commenters noted that the requirements for penetration testing are overly prescriptive or burdensome, while another commenter questioned what the Coast Guard's expectation was for penetration testing.

The regulation provides minimum baseline cybersecurity requirements. The Coast Guard does not agree that the penetration testing requirements are overly prescriptive. The requirements in § 101.650(e)(2) do not dictate the scope of the test but, instead, state that the owner or operator or designated CySO of a U.S.-flagged vessel, facility, or OCS facility must only ensure that a penetration test has been completed.

Some commenters requested clarification on multiple aspects of the penetration testing requirements, including whether the frequency is linked to the renewal of a VSP, FSP, or OCS FSP.

The Coast Guard revised § 101.650 in this final rule to clarify that penetration testing must be completed in conjunction with renewing the

Cybersecurity Plan. Furthermore, the owner or operator has the discretion to determine who has the capabilities to perform a penetration test. If personnel on the U.S.-flagged vessel, facility, or OCS facility have the technical expertise, penetration testing can be done internally. If personnel on the U.S.-flagged vessel, facility, or OCS facility do not have such technical expertise, then an external organization must conduct the penetration testing.

One commenter noted that not every cybersecurity incident has the potential to result in a TSI. The requirement to report threats could be arbitrary and overly burdensome, especially given the influx of reports from multiple threat vectors. One commenter requested that the Coast Guard adjust the language for what information the regulated entity is required to submit for the penetration test and suggested that owners and operators should provide the Coast Guard a letter certifying that a penetration test was conducted. This approach simplifies reporting expectations for the industry while alleviating pressure on the NRC.

The Coast Guard's definition of a reportable cyber incident in this final rule includes, among other things, ''Incidents that otherwise may lead to a transportation security incident'' which 33 CFR 101.105 defines as ''a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.'' The Coast Guard feels that the scope of this definition allows stakeholders to report a cybersecurity incident they reasonably identify as potentially leading to a TSI but also includes other types of cybersecurity incidents that would not require the entity estimate TSI risks. The scope of the definition also helps ensure the Coast Guard receive sufficient information so that it can best evaluate the risk of TSI and, in turn, coordinate any necessary response. It is likely the Coast Guard will be better positioned than a single regulated entity to evaluate the available facts, especially in circumstances when multiple entities are affected.

The Coast Guard has also issued, and will update as needed, guidance on incident reporting in the form of a NVIC. If there is a question as to whether an incident would meet these criteria, a regulated entity may report to the NRC, or they may notify their local Captain of the Port for guidance.

The Coast Guard notes that the requirements to report cybersecurity incidents in accordance with this final rule are satisfied by entities that are also covered by 33 CFR part 6 and report pursuant to 33 CFR 6.16–1. The Coast Guard recognized, based on public comments, that stakeholders would be best served with clear guidance on what would be required for submission to verify the penetration tests. The Coast Guard agreed that a letter verifying that the test was conducted, while noting any identified vulnerabilities, would represent a minimal burden on industry regarding submission requirements.

We revised § 101.650(e)(2) to specify that the CySO must submit a letter verifying that the test was conducted, as well as all vulnerabilities identified from the penetration testing. Additionally, the Coast Guard will consider developing a letter template as part of future guidance that will further assist stakeholders in meeting requirements. This information must be included in the Vessel Security Assessment (VSA), FSA, or OCS FSA, according to 33 CFR 104.305, 105.305, and 106.305. Further documentation related to the penetration tests must be made available to the Coast Guard upon request as required by § 101.660.

One commenter inquired if it would be possible for the owner or operator to apply for an exemption to the penetration test if there are not any major modifications during the 5 years in between penetration tests.

Each situation will be evaluated on its own merits on a case-by-case basis. Regulated entities may discuss specific concerns with the cognizant COTP, OCMI, or the MSC, as appropriate. The Coast Guard provides procedures in § 101.665 for an owner or operator to request a waiver or equivalence determination for the requirements.

One commenter asked if the Coast Guard would accept penetration testing of the same architecture but in a lab environment in light of the safety and operational risks active vessels face while conducting penetration testing on a voyage. The commenter noted that many vessels typically do not stop for prolonged periods of time. The commenter also asked if penetration testing of the IT environment could be limited to noncritical systems.

The Coast Guard understands the concern about conducting penetration testing on voyages. If an owner or operator of a U.S.-flagged vessel, facility, or OCS facility believes that their method of compliance with these regulations is outside of the stated requirements, or believes the requirements are not applicable to certain operations, they may request a waiver or equivalency according to the procedures in § 101.665. For example, if the organization wants to conduct the penetration testing in a lab environment, they can request an equivalent and explain how the lab environment satisfies the stated requirements in their case. In some cases, a temporary waiver may be appropriate. In terms of whether penetration testing could be limited to non-critical systems, if an owner or operator believes that penetration testing of their IT environment could be limited to noncritical systems, then they may request a waiver or equivalency according to the procedures in § 101.665.

One commenter noted that penetration testing should be considered a method of conducting a Cybersecurity Assessment and that penetration testing should be conducted with the audit as an assessment every several years, or as needed by the facility.

In this final rule, the Coast Guard considers penetration testing, Cybersecurity Assessments, and audits to be distinct actions. They are not interchangeable, and each serves specific functions as part of the comprehensive cybersecurity requirements of this final rule. These are separate and distinct actions ranging from less technical to very technical. Audits are on the less technical side. Audits serve to determine the accuracy and validity of a document against any potential changes since the last review, and usually include a review of policies, procedures, and records. Cybersecurity Assessments assist in identifying actual or potential vulnerabilities, whether new, evolving, or pre-existing, in a regulated entity's IT and OT systems, equipment, and procedures, so that the stakeholder can then address such vulnerabilities in a Cybersecurity Plan. Assessments also generally help ensure that policies and procedures are followed and verify that automated process are completed according to those policies and procedures (for example, whether patching was deployed accordingly). Penetration testing is a more technical test of the entity's cybersecurity to see what an outside cyberattack or inside threat could do. It may uncover gaps that an Assessment may not. The owner or operator of a U.S.-flagged vessel, facility, or OCS facility may choose, but is not required, to conduct the penetration testing in conjunction with a Cybersecurity Assessment and an audit.

R. Comments Related to Supply Chain (§ 101.650(f))

One commenter suggested that the Coast Guard not use the term ''breach''

when referring to incidents requiring reporting of a cyber incident by vendors to owners or operators. Other commenters indicated that any requirement for a vendor or service provide to notify a regulated entity of vulnerabilities or incidents was not practical.

The Coast Guard revised § 101.650(f)(2) to remove the references to ''breaches'' and ''incidents'' and replaced them with ''reportable cyber incidents,'' consistent with the decision to define and use that term in these regulations. It is our position that it is appropriate to require owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to establish a process for receiving information from vendors and third parties to best address potential threats and vulnerabilities. The Coast Guard recognizes that, with any cybersecurity vulnerability or incident, it may not be discovered immediately, and in fact, it could be any length of time before it is discovered, whether by the regulated entity itself or by a vendor, third party, or other entity. Vendors and third parties often have a significant role in an entity's operations, and in cases when they impact a regulated entity's IT and OT systems and equipment, it is vital to address this as a potential source of a cybersecurity threat and vulnerability. The Coast Guard believes that ignoring the potential cybersecurity impact of vendors and third parties is to ignore an identified threat vector.

The Coast Guard does not feel it is an undue burden to require regulated entities to incorporate a requirement in contracts or other agreements with vendors and third-party services that when a partner identifies a cybersecurity vulnerability or incident, they must notify regulated entities that could likewise be adversely impacted. Without requiring a notification when a vendor or third-party service provider is aware of an issue but there is no mechanism for their service partners to be made aware, our regulated entities are potentially subject to cybersecurity vulnerabilities and incidents for which they might otherwise be able to take more timely action to prevent, mitigate, and respond.

One commenter asked if there would be a list of approved vendors for equipment, services, and assessments.

The Coast Guard does not plan to provide a list of ''approved'' vendors. Owners or operators may choose those vendors that best meet their individual needs, which may not be the same for every organization. One commenter requested additional clarity regarding what information or capabilities are required of vendors and third-party contractors when providing services to vessels, facilities, and OCS facilities.

The Coast Guard does not determine what requirements or criteria a specific vendor, supply-chain provider, or other third party must meet. This final rule requires that owners and operators consider cybersecurity capabilities. It is up to the owner or operator of a U.S.-flagged vessel, facility, or OCS facility to determine whether a provider meets the requirements that best support their operations and what they feel are the necessary capabilities to safely and securely support their business operations.

One commenter suggested that the Coast Guard provide broad oversight of vendors that provide critical services to broad spectrums of the maritime industry.

This final rule applies to owners or operators of U.S.-flagged vessels, facilities, and OCS facilities who will need to select vendors or third parties based on their own criteria and to ensure regulatory requirements are met. The commenter's suggestion is outside the scope of the rulemaking. The Coast Guard will not create or maintain a list of approved vendors.

One commenter stated that the requirement for owners or operators to analyze all networks to identify vulnerabilities to IT and OT systems and the risks posed by each digital asset was overly burdensome, particularly because of the words ''all'' and ''each.''

The Coast Guard revised § 101.650(e)(1)(i) to clarify that the owner or operator of a U.S.-flagged vessel, facility, or OCS facility must analyze all networks to identify vulnerabilities to critical IT and OT systems, consistent with our definition and use of the term *critical IT and OT systems* throughout this final rule.

S. Comments Related to Resilience (§ 101.650(g))

One commenter suggested we require backups of critical IT and OT systems ''periodically'' as opposed to ''frequently.''

The term ''frequently'' in § 101.650(g)(4) emphasizes a timely review and the need to keep up with the rapidly evolving threat landscape that cybersecurity poses to the MTS. It is up to the owner or operator of a U.S.-flagged vessel, facility, or OCS facility to interpret ''frequently,'' develop a schedule that is appropriate for their organization, and document it in their Cybersecurity Plan. For these reasons, we did not make a change in response to this comment.

One commenter suggested that requirements for backups should include testing of restore processes for operations-critical systems and data annually.

The requirements for backups in this final rule are sufficient as minimum baseline requirements. Owners or operators of U.S.-flagged vessels, facilities, and OCS facilities are welcome to take additional measures as appropriate to their systems, equipment, and operations. For this reason, we did not make a change in response to this comment.

T. Comments Related to Network Segmentation (§ 101.650(h))

One commenter noted that the network segmentation requirements are too prescriptive, while other commenters recommended a ''standards-based, technology-neutral approach.''

The Coast Guard notes that the network segmentation requirements in § 101.650(h) provide minimum baseline standards while allowing an owner or operator of a U.S.-flagged vessel, facility, or OCS facility flexibility in conducting the segmentation. Regulated entities may discuss specific concerns with the cognizant COTP, OCMI, or MSC, as appropriate. When deviations must occur or equivalency to other cybersecurity standards are proposed, the owner or operator may file a waiver or equivalency request according to the procedures in § 101.665.

U. Comments Related to Cybersecurity Compliance Dates (§ 101.655)

Some commenters recommended that the Coast Guard extend the implementation period and compliance dates for the cybersecurity requirements in this final rule beyond the 12 to 18 months that we proposed in the NPRM. For example, one commenter asked the Coast Guard to allow an implementation period of 36 to 48 months following the effective date of a final rule. The commenter believed that the proposed implementation period would be insufficient because cybersecurity programs require more time to mature. The commenter stated that 36 to 48 months would afford sufficient time for owners and operators to comply. Another commenter requested that a phased schedule be developed to allow time to implement the proposed regulations. Another commenter stated that six months is not a sufficient amount of time for a vessel operator to develop a Cybersecurity Plan and develop and implement cybersecurity training on that Cybersecurity Plan. The commenter recommended that the Coast

Guard extend the deadline for completion of cybersecurity training to the date 365 days after the effective date of the final rule.

The Coast Guard does not agree with the suggestion to delay the overall implementation by 36 to 48 months, but has implemented a phased implementation period for all regulated entities. Under this rule, the regulatory text will take effect, and reporting requirements under this rule will commence, 180 days after publication. Training requirements are due 180 days thereafter, followed by a 24-month implementation period for the rule's requirements to conduct a Cybersecurity Assessment, submit a Cybersecurity Plan, and designate a CySO. We believe that this approach, which results in a one-year lead time for cybersecurity training accounts for the need for action to address continually evolving cybersecurity threats and vulnerabilities, and provides regulated entities with adequate time to comply with this final rule and address its requirements.

We revised § 101.650(e)(1) to specify that owners and operators will need to conduct the Cybersecurity Assessment within 24 months of the effective date of this final rule. The Cybersecurity Plan must also be submitted to the Coast Guard for review and approval within 24 months of the effective date of this final rule, rather than during the second annual audit following the effective date, as stated in the NPRM. We revised § 101.655 to reflect this change. We note that in Section VII of this preamble, we are requesting public comment on a potential 2-to-5-year delay for the implementation periods for U.S.-flagged vessels.

The Coast Guard has declined to phase in implementation based on a specific organization's audit date, in order to ensure that owners and operators are generally on equal footing with respect to the amount of time in which to implement these requirements. Owners and operators who prefer to align their Cybersecurity Plans with existing plans may submit their required Plans at any time before the 24-month deadline. Additionally, owners and operators may contact the cognizant COTP or OCMI for facilities or OCS facilities or the MSC for U.S.-flagged vessels, or follow the procedures for requesting a waiver, equivalence determination, or temporary permission under § 101.665 if more time is needed to comply with the requirements.

V. Comments Related to Cybersecurity Compliance Documentation (§ 101.660)

Some commenters expressed concern about portions of the Cybersecurity Plan being submitted to the Coast Guard, with the information being at risk of inadvertent release. The commenters believed this could unnecessarily expose participating entities to cybersecurity threats, inconsistent outcomes, foreseeable delays, and additional effort.

The Coast Guard understands the concerns with submitting information that could put a U.S.-flagged vessel, facility, OCS facility, or organization at risk of cybersecurity threats. However, the Coast Guard regularly handles sensitive information and does not agree that submitting Cybersecurity Plans will result in inconsistent outcomes, foreseeable delays, additional effort, or risk. If an owner or operator has concerns about submitting a specific section or portion of their Cybersecurity Plan, they may discuss these concerns with the cognizant COTP, OCMI, or MSC, who will work with the regulated entity to determine whether certain information could be submitted directly or made available to the Coast Guard through other means. The Coast Guard will also continuously evaluate any such concerns and feedback and, if necessary, provide amplifying guidance to all regulated entities as well as Coast Guard personnel to ensure uniform application of the requirements. While the Coast Guard will always emphasize consistency, it is noted that each entity's Plan will be assessed individually, and differences may result based on the regulated entity's specific Plan and cybersecurity needs.

One commenter stated that they believed that cybersecurity records should not be maintained on board a vessel but would be best kept shoreside. Another commenter recommended vessels follow processes similar to the International Convention for Safety of Life at Sea, 1974 (SOLAS) rules, where an RO system is already in place.

These regulations do not prescribe where the records need to be kept but do require that they be made available to the Coast Guard upon request. Each owner or operator may determine where their records are best secured, according to 49 CFR part 1520, and how to ensure the records can be made readily available to the Coast Guard upon request. So long as it meets these requirements, an owner or operator may choose to use an existing system, where appropriate.

One commenter expressed concerns about the level of details included in documentation of penetration testing. They believe that this information should be made available to the Coast Guard only with reasonable cause.

The Coast Guard does not agree with the commenter's assertion that required documentation under these regulations should be made available only with reasonable cause. This final rule allows for certain documentation to be maintained by the owner or operator, and to be made available to the Coast Guard upon request, as required by § 101.660, so that Coast Guard can ensure compliance with the regulations. Regarding the requirements for penetration testing, we revised § 101.650(e)(2) in this final rule to specify that following the penetration test, a letter certifying that the test was conducted, as well as all identified vulnerabilities, must be included in the VSA, FSA, or OCS FSA, according to 33 CFR 104.305, 105.305, and 106.305.

One commenter requested that these regulations include a mechanism for industry to share information and best practices with each other.

In § 101.650(e)(3)(iii) for routine maintenance, we require the owner or operator to maintain a method to share threat and vulnerability information with external stakeholders. We do not prescribe the particular mechanism and, instead, leave that to the discretion of the individual owners and operators.

One commenter recommended that the completed Cybersecurity Assessment, along with approval from vessel's master, facility manager, and port master be retained for a specified duration, as well as any action plan designed to reduce the residual risk.

The Coast Guard provides minimum baseline recordkeeping requirements for regulated entities in these regulations. As such, we are not specifying a minimum duration for retention of completed Cybersecurity Assessments by the regulated entity. Owners or operators may impose additional recordkeeping requirements if they desire.

One commenter suggested that the Coast Guard require ''Management of Change'' in documentation requirements.

The Coast Guard believes that ''Management of Change'' documentation is an internal process issue for the owner or operator, and that it is unnecessary to address it in these regulations. Each owner or operator should make their own determination as to whether and how they address their Management of Change processes and procedures.

One commenter acknowledged the importance of maintaining cybersecurity

documentation as required by this regulation, and the need to have the documentation made available to the Coast Guard upon request. They requested additional information as to how the Coast Guard will conduct its reviews of the documentation.

The Coast Guard cannot provide specifics about its procedures in conducting cybersecurity documentation reviews based on this final rule, as each situation will be handled on a case-by-case basis, starting with the local COTP.

W. Comments Related to Noncompliance, Waivers, and Equivalents (§ 101.665)

One commenter noted that some systems on board their facilities are fully managed by the system vendor, and modifying these systems to meet new regulations might affect the warranty and support of these systems. They questioned who is ultimately the accountable party for vendor-managed systems.

Owners and operators are ultimately responsible for the systems and equipment at their U.S.-flagged vessel, facility, or OCS facility. They should work with vendors to identify what security measures are in place that could meet the requirements of these regulations, or how they will adjust ensure systems and equipment are secured. Additionally, we have added language for the procedures for noncompliance, waivers, and equivalents with regulatory compliance.

One commenter requested that the Coast Guard provide a form of credit, equivalence, or exemption to owners and operators who already have similar structures in place to comply with these regulations. Some commenters asked about the ability to request alternative compliance methods.

The Coast Guard does not provide a blanket credit, equivalence, or exemption based on a regulated entity's compliance with similar regulations or requirements. An owner or operator of a U.S.-flagged vessel, facility, or OCS facility may use those structures to inform their Cybersecurity Assessment, Cybersecurity Plan, and compliance with this final rule and, as needed, may follow the procedures in § 101.665 to request a waiver or equivalence determination. When compliance with similar or parallel regulations or requirements is the basis for an owner or operator to request a waiver, the Coast Guard notes that the owner or operator must still detail the portions of the Coast Guard's regulation they meet, and the specific measures taken under that similar or parallel compliance when requesting a waiver or equivalency. An owner or operator simply stating that they are complying with equivalent measures does not provide the Coast Guard with enough information to ensure regulatory compliance.

Some commenters requested the Coast Guard exempt facilities subject to the TSA's Pipeline Security Directives or otherwise clarify the applicability of facilities subject to both this final rule and the Security Directives.

TSA's Pipeline Security Directives are issued under separate authorities and with a separate purpose from these regulations. This final rule establishes baseline cybersecurity requirements for a broader segment of the maritime industry than the entities under the Pipeline Security Directives. Stakeholders subject to this final rule that believe there is an overlap between agencies' requirements, stakeholders may use their compliance measures for the other requirements (for example, TSA's Pipeline Security Directive) to inform their compliance with the Coast Guard's cybersecurity requirements in this final rule. The Coast Guard may seek documentation that demonstrates to the Coast Guard how they are implementing the other agencies' cybersecurity requirements. Stakeholders may also submit a request for waiver or equivalency according to § 101.665 of this final rule.

X. Comments Related to Costs

Several commenters stated that Coast Guard underestimated the supply chain costs related to monitoring and that additional employee(s) may be necessary.

The Coast Guard decided not to estimate costs for § 101.650(f)(1) and (f)(2) because owners and operators would need to consider cybersecurity capabilities only when selecting third-party vendors for IT and OT systems or services. In addition, we assumed most third-party providers have existing cybersecurity capabilities and already have systems in place to notify the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities of any cybersecurity vulnerabilities, incidents, or breaches that take place. Therefore, we assume the commenter is primarily referring to our cost estimate for § 101.650(f)(3), which requires owners and operators to monitor and document all third-party remote connections to detect cyber incidents.

While we include costs for documenting remote third-party connections when developing the Cybersecurity Plan and costs for annual maintenance, we did not include a separate cost estimate for monitoring those connections but instead noted them as unquantifiable costs. The Coast Guard acknowledges that this could take additional time, mostly through reviewing logs for remote connections. The amount of time this could take is dependent on the size of the organization, making accurate estimates difficult. However, we disagree that most owners or operators will need to hire additional employees, since many affected entities are considered small (see our Final Regulatory Flexibility Analysis (FRFA)) and likely do not have complex networks that would require full-time active monitoring. Estimating costs associated with the hiring of a full-time employee would represent a severe overestimate for many of the small owner and operators affected by this final rule, and we have decided not to include those costs in the RA.

Several commenters stated that the Coast Guard underestimated the costs related to the required device security measures and that costs may ''balloon'' with each additional vessel, facility, or OCS facility owned or operated.

In our efforts to capture the costs related to device security measures outlined in § 101.650(b), the Coast Guard considered those measures as a part of the overall Cybersecurity Plan development and included any associated hour burden in the estimated hour burdens associated with Cybersecurity Plans. The Coast Guard acknowledges that these items take time, but we believe our hour-burden estimates reflect averages for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities of various types and sizes in the affected population, based on information and data from several different sources that we outlined in the *Cybersecurity Measure Costs* section of this RA.

Regarding the commenter's suggestion that the cost may balloon with each additional U.S.-flagged vessel, facility, or OCS facility, we estimated Cybersecurity Plan costs for each facility and OCS facility rather than for the owner or operator of a facility or OCS facility in the affected population, as explained in the RA. However, for owners and operators of U.S.-flagged vessels, we assumed that a CySO will not need to expend a great deal of additional time developing a Cybersecurity Plan for each U.S.-flagged vessel owned by a U.S.-flagged vessel company. We believe it is more likely that the CySO will create a master Cybersecurity Plan for all the U.S.-flagged vessels in the fleet, and then tailor each Plan according to a specific U.S.-flagged vessel, as necessary.

Because a large portion of the provisions required under this final rule will 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 U.S.-flagged vessels owned by the same owner or operator.

Similarly, we assume that much of the IT and OT technology on board the affected U.S.-flagged vessels will be consistent across vessels in the same fleet, making estimates that balloon with each additional vessel owned prone to overestimation. As a result, the Coast Guard decided to maintain its current cost estimates for the device security measures outlined in § 101.650(b) as part of the Cybersecurity Plan development and maintenance, barring the availability of any specific data from the affected population.

Several commenters stated that the costs related to penetration testing were grossly underestimated. Another commenter who represents operators of offshore supply vessels (OSVs) stated that our estimates failed to consider the costs associated with the additional internet protocol (IP) addresses [59] connecting to networks from industrial personnel, employees with multiple devices, and OT systems.

To estimate costs related to penetration testing, the Coast Guard used estimates provided to us by NMSAC members and Coast Guard SMEs with experience contracting for and performing penetration tests. We also relied on the Jones Walker survey,[60] which is a publicly available survey of the portion of facilities that currently conduct penetration testing. Our goal was to use an average estimate based on real world data. We also attempted to include some variability to capture increased costs for larger sized organizations by basing a portion of the cost on the number of IP addresses or employees in an organization. Though we did not receive additional estimates or data on real costs incurred by members of the affected population via public comments, we have adjusted our cost estimate for penetration testing. We base our adjustments on suggestions from public commenters who stated that we underestimated costs and failed to account for all IP addresses along with additional information collected from SMEs, who have experience performing penetration tests. With this additional data, we doubled our estimate of the initial penetration testing cost from $5,000 in the NPRM to $10,000 for the final rule, the cost per IP address from $50 in the NPRM to $100 for the final rule, and the number of IP addresses per organization, which is now based on the number of employees in an organization multiplied by 2. Please see the *Penetration Testing* section of the RA to see the impact of these changes on our cost estimates in the final rule for U.S.-flagged vessels, facilities, and OCS facilities.

One commenter stated that Coast Guard underestimated the cost of routine system maintenance, and that additional employee(s) may be necessary to perform the actions.

Concerning cost estimates related to routine system maintenance, the costs associated with § 101.650(e)(3)(i) through (v) are included in the costs for conducting a Cybersecurity Assessment and developing a Cybersecurity Plan. For § 101.650(e)(3)(vi), we included a separate cost for the annual subscription cost of a vulnerability scanner. The Coast Guard acknowledges that the patching in paragraph (e)(3)(i), monitoring for submitted vulnerabilities in paragraph (e)(3)(ii) and scanning for vulnerabilities in paragraph (e)(3)(vi) could require additional time to monitor in some circumstances, mainly related to OT systems. However, the Coast Guard disagrees that this is true for most of the affected population. Patching for IT systems can be set to automatically update and download without much risk, and vulnerability scans are typically background processes that only need monitoring in the event of an alert or incident. Patching for OT systems may be more complicated to allow for automatic updates, but the Coast Guard lacks data on how prevalent these systems are in the affected population, and how much time this could take. The estimates we used for the monetized portion of this provision in § 101.650(e)(3)(vi) are based on information from CGCYBER and NMSAC, as we outlined in the *Routine System Maintenance for Risk Management* section of this RA. As such, we do not anticipate the need for these items to require a full-time employee for most owners or operators in the affected population, and we are unable to adjust the cost estimates without more specific data provided to us through public comments.

Several commenters stated that the costs for drills and exercises were underestimated. Some commenters stated that the costs for drills were underestimated because the cybersecurity drills could not be rolled into existing drills. Further, multiple commenters stated that the CySO is not the only individual that would be involved, and so costs for other personnel should be included in the calculations. Another commenter stated that our estimates in the NPRM failed to take into account the costs of training personnel to supervise drills, documenting the conduct of drills, identifying lessons learned, and disseminating information to employees. Another commenter encouraged the Coast Guard to consult vessel operators to develop a more accurate understanding of the time burden and costs associated with drill development. Other commenters also requested that the Coast Guard reduce the frequency of drills, with some requesting a general frequency reduction, others requesting annual or semi-annual drill requirements, and others requesting a schedule of requirements based on the cybersecurity risk faced by the affected U.S.-flagged vessels and facilities.

Another comment, from trade associations representing nearly 750 MTSA regulated facilities, stated that they disagreed with the Coast Guard cybersecurity exercise estimates that did not require additional time from participants. The commenters disagreed that these new cyber exercises could be easily combined with existing security exercises because they are similar in scope and size. According to the commenter, to combine both would require the exercise to test more subject matter, and result in longer exercises requiring more participant time and preparation.

The Coast Guard agrees with suggestions from commenters that costs have been underestimated for drills and exercises if they are not combined with existing drills and exercises. As mentioned by multiple commenters, requiring drills and exercises at the same interval as physical security drills and exercises already required in 33 CFR parts 104, 105, and 106 facilitates the combination of cybersecurity and physical security drills, and this is still allowed in the final rule. However, we accept the points raised, which were shared by several other commenters, that cybersecurity drills and exercises

[59] An IP address is a unique numerical identifier for each device or network that connects to the internet.

[60] 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 RA. Readers can access the survey at *https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html,* accessed August 16, 2024.

are not always easily combined with physical security drills and exercises given the scope and material being tested. The Coast Guard acknowledges that employees beyond the CySO will need to participate in the drills and exercises in instances where they are not combined. For the purposes of our RA of this final rule, we now assume that no owners or operators will combine their cybersecurity drills or exercises with existing drills or exercises, and that a certain portion of employees at the organization will participate in the new drills and exercises.

Based on new information from Coast Guard SMEs in the Office of Port and Facility Compliance (CG–FAC) and the Atlantic Area (LANTAREA), we have adjusted our cost estimates to reflect 8 hours for drill development and 4 hours for drill participation for participating employees. Because our estimated costs are now higher due to the increased hour burden estimate per drill, and based on public commenter suggestions, we have reduced the frequency of the cybersecurity drill requirement from quarterly to at least 2 drills every 12 months, to relieve the burden on owners and operators. Upon review and consideration of comments, the Coast Guard recognizes that regulated entities can assess their cybersecurity risks and vulnerabilities and the status of their cybersecurity measures through 2 drills every 12 months instead of more frequent occurrences. While there are benefits of a more robust drill schedule, we believe that this reduction in the number of drills lowers costs and increases marginal benefits by allowing affected owners and operators to use resources that would have been directed to those drills to improve remaining drills or implement cybersecurity measures that can help reduce the risk of a cyber incident in other ways. Further, by having fewer drills to develop and conduct, we believe the remaining drills will be less superficial, which one commenter remarked was a concern with previously proposed frequency cybersecurity drills. However, the Coast Guard believes that anything less frequent than two drills per year could lead to a decrease in focus on the issues that a drill would emphasize. This is especially true with regard to cybersecurity, as risk and vulnerabilities can change rapidly over the course of a year.

In addition, we have adjusted our cost estimates for exercises to reflect 20 hours for exercise development and 4 hours for exercise participation for participating employees. According to § 101.635(a), drills and exercises must test the proficiency of the U.S.-flagged vessel, facility, and OCS facility personnel in assigned cybersecurity duties. Because we do not have data on which portion of a given owner or operator's employees will have cybersecurity responsibilities, we use the estimated 33 percent ''shoreside'' share of employees for vessel owners and operators, and the same percentage of employees for facility and OCS facility owners and operators, to estimate the costs associated with drill and exercise participation. We feel this is in line with the requirements of the regulatory text and suggestions from a commenter who stated that ''onboard personnel have little to no involvement in cyber specific drills.'' Please see the *Drills and Exercises* sections of the RA to see the impact of these changes on our cost estimates for U.S.-flagged vessels, facilities, and OCS facilities.

Several commenters stated the Coast Guard underestimated costs associated with network segmentation.

The Coast Guard acknowledges a challenge in estimating costs for network segmentation. As mentioned in this RA, network segmentation can be particularly difficult in the MTS, because of the age of infrastructure in the affected population of U.S.-flagged vessels, facilities, and OCS facilities. The older the infrastructure, the more challenging network segmentation may be. Given this, and the amount of diversity regarding the state of infrastructure across the various groups in our affected population, we are not able to fully estimate the compliance costs associated with this provision. We also did not receive any additional information or data from commenters that could be used to help us improve our estimate of the potential costs for network segmentation, which represented one of the largest sources of uncertainty in the RA. Therefore, we retained the original estimates from the NPRM for this provision.

In accordance with OMB Circular A–4, uncertainty analysis is a tool that can be used by Federal agencies to present uncertainty associated with the estimation of costs, sources of data, and more, in an RA. In table 42 of the RA, we list uncertainties related to the economic impact of certain provisions of this final rule, including the state of infrastructure for network segmentation. In some cases, we list a range of potential cost estimates, if a point estimate was not available for use in the RA. For other provisions of this final rule, where we received additional data or information from commenters, we used this information and updated our estimate of costs and burden hours, if applicable, in the RA.

One commenter stated that the affected population counts used in the NPRM for U.S.-flagged vessels regulated under subchapters H and K were inaccurate and provided updated numbers. According to the comment, the affected populations listed in table 6 of the NPRM for vessels inspected under 46 CFR subchapter H (34 vessels) and subchapter K (379 vessels) are too low. The commenter cited the USCG—PVA Quality Partnership Annual Report for the years 2021–2023, which indicated that there are 136 vessels inspected under 46 CFR subchapter H and 428 vessels inspected under subchapter K that would be subject to the cybersecurity requirements.

The Coast Guard thanks the commenter for noting the discrepancy in the population for U.S.-flagged vessels under subchapters H and K. We inadvertently removed certain public vessels that are included under the applicability of this final rule, or in ''Applicability'' in 33 CFR 101.605, which resulted in the error. Therefore, we now estimate the revised population for U.S.-flagged vessels under subchapters H and K to be approximately 131 and 430, respectively, based on our updated population data we obtained from our Marine Information for Safety and Law Enforcement (MISLE) database. These figures are only slightly different from those highlighted in the USCG–PVA Quality Partnership Annual Report for the years 2021–2023, which we assume is the result of small year-to-year changes in vessel populations. As a part of this update, we also updated all our other affected population data. Readers can view the section, *Affected Population,* and table 6 in the RA.

Several commenters stated that a there is a substantial additional cost to contract cybersecurity services or hire additional staff based on the estimates provided in the RA.

The Coast Guard thanks the commenter for raising the concern. However, in § 101.625 of this final rule, we do not require any owner or operator of a U.S.-flagged vessel, facility, or OCS facility to hire a dedicated CySO to perform the duties stated in this part or in § 101.630 for the Cybersecurity Plan. In the *Cybersecurity Plan Costs* section of the RA, we state that a CySO can be an existing person within a given organization who may perform the duties and assume the responsibilities of a CySO provided that this person can maintain their current responsibilities within the organization. Therefore, an organization has the flexibility to

determine if an existing employee such as a VSO, FSO, or CSO can perform the functions of a CySO. Despite this, we acknowledge that some owners or operators may need to hire a CySO if no existing employees are able take on these duties. However, rather than estimating the hours associated with bringing on a full-time employee, the hour burdens associated with CySO duties have been quantified in various sections of the cost analysis. This can capture the costs associated with contracting for the individual CySO duties or assigning them to a new or existing employee.

One commenter stated that we miscategorized the role of the CySO under the ''Information Security Analyst'' category, rather than using a CISO. The commenter also suggested that it is unlikely a single individual could perform all the required functions, indicating an underestimation of costs and management overhead. The commenter also noted that U.S. maritime academies currently lack curriculum for producing maritime cybersecurity professionals, making it difficult to fill CySO positions with qualified personnel. As a result, the commenter urged the Coast Guard to engage with public and private maritime academies to address a lack of qualified personnel.

The Coast Guard disagrees with the assertion that we have miscategorized the CySO role. A CISO, as the commenter suggests, is typically a C-suite or executive-level management position. While it is acceptable for affected entities to hire or designate an existing CISO as the CySO to comply with this final rule, it is not required. We believe that the roles and responsibilities assigned to the CySO role are of a smaller scope and scale than what would typically be expected of a C-suite level CISO, and that estimates in line with typical CISO wages would greatly overestimate the costs of this final rule for owners and operators of smaller U.S.-flagged vessels, facilities, and OCS facilities.

We believe the same is true for the claim that multiple individuals would need to take on the CySO duties. Assuming multiple personnel would result in overestimates for most small entities with less comprehensive cybersecurity programs and risks. Therefore, we used the estimates that we believe best reflect the average burden for the affected entities.

In order to have as large a population of CySOs as possible, graduation from a maritime academy, or having a Merchant Mariner Credential (MMC), is not required. Cybersecurity systems in the maritime industry are not so unique from other industries as to require specialization in MTSs. An MMC would be required only if the CySO's duties, as required by the company and its Cybersecurity Plan, require additional duties in a location, such as on a vessel, would otherwise require an MMC. CySOs, like VSOs, FSOs, or OCS FSOs, require only general knowledge of their company's maritime operations. The Coast Guard has no plans to create a CySO MMC. If maritime academies wish to develop CySO training programs so a graduate earns an MMC along with CySO credentials, they are encouraged to develop such programs.

One commenter stated that the cost for the commercial shipping sector is substantial, especially for smaller vessel owners and operators in an economic environment that has tight margins and substantial risk.

The Coast Guard acknowledges that this final rule will create significant costs for affected small entities, based on our FRFA, but it will also create significant benefits for the affected entities and the maritime industry as a whole. In several areas of this final rule, we referenced CEA's 2018 report (see the III. Basis and Purpose and the *Benefits* sections of the preamble and RA, respectively) on the state of cybersecurity in the marketplace and how firms viewed cybersecurity or behaved when faced with cybersecurity challenges. In support of this final rule, we provided excerpts from this report, which in part state that firms ''[r]ationally underinvest in cybersecurity relative to the socially optimal level'' and ''[i]t often falls to regulators to devise a series of penalties and incentives to increase the level of investment to the desired level.'' [61] With this understanding, we formulated minimum cybersecurity requirements that may assist firms and regulated entities with their cybersecurity posture in an effort to reduce the likelihood, vulnerability, and risk of a cyber incident. If a cyber incident occurs, the Coast Guard believes that the minimum cybersecurity requirements will mitigate its impact on firms, and regulated entities, and the U.S. economy, and create the intended benefits for the regulated entities.

In table 51 of the RA, we list the potential benefits of this final rule, and ones specifically related to cybersecurity measures for firms where we state, ''A cyber-resilient organization can maintain or quickly resume operations in the event of a cyber-attack, minimizing downtime and ensuring that essential services remain available to customers and stakeholders. This reduces the potential for costly disruptions to maritime operations,'' and reduces the downstream impacts to ''economic participants.'' Generally, firms with strong cybersecurity measures will have benefits that include improved preparedness, reduced vulnerability, improved data protection, reduced risk of reportable cyber incidents, improved training, improved incident response, and enhanced trust with economic partners, among many others we listed.

In our consideration of public comments in the FRFA, we state that we will provide assistance to small entities through reducing the required frequency of cybersecurity drills from quarterly to twice annually, extending the implementation period and compliance dates for the Cybersecurity Assessment and Cybersecurity Plan in this final rule to 24 months rather than the 12 to 18 months that we proposed in the NPRM. By using the same implementation period for each group of regulated entities rather than basing this on the organization's audit date, the relevant owners and operators will have the same amount of time in which to implement these requirements, and in many cases will have additional time to come into compliance when compared to the NPRM. Please see our Small Entity Compliance Guide, which is available in the docket, for additional help regarding how small entities can best comply with this final rule.

One commenter stated that the time requirement for updates under § 101.630 may be unrealistic due to vessels that are operating internationally with limited access to materials or equipment.

The Coast Guard understands that each U.S.-flagged vessel, facility, and OCS facility operates facing different cybersecurity risks. Owners and operators may seek an equivalency or waiver by following the procedures in § 101.665. This flexibility is intended to accommodate varying levels of risk and operational needs across different vessels, facilities, and OCS facilities. We revised § 101.630(e)(1)(ii) to clarify that the owner and operator will have at least 60 days to submit its proposed amendments. Further, we have revised § 101.655 to reflect that the Cybersecurity Plan must be submitted to the Coast Guard for review and approval within 24 months of the effective date of this final rule, rather than during the second annual audit following the effective date. In addition, we revised § 101.650(e)(1) to specify that owners

[61] Economic Report of the President *supra* note 2 at 323–24.

and operators will need to conduct the cyber assessment within 24 months of the effective date of this final rule, an increase from 12 months proposed in the NPRM. All these revisions should give owners and operators more time and flexibility to comply with this final rule.

One commenter stated that the Coast Guard failed to delineate costs between OCS and waterfront facilities in the RA, leading to potentially inaccurate cost estimates for the 33 OCS facilities operated by 9 different entities. In addition, the commenter stated that the Coast Guard failed to acknowledge the traditional costs for inspection of OCS facilities, including the commercial helicopter contract used to reach the OCS facility platforms.

The Coast Guard acknowledges that OCS facilities were grouped in with the waterfront facilities in the RA in the NPRM. The Coast Guard believes that the cost estimates for compliance with this final rule are similar across waterfront facilities and OCS facilities. Nonetheless, for greater clarity, in the RA for this final rule we highlight the specific OCS-related cost estimates for OCS facilities as a subset of the overall facility cost estimates, at the end of each section of the analysis.

Regarding the inspection costs for OCS facilities, we included cost estimates for the marginal increase in onsite inspection time for the population of facilities and OCS facilities. 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 final rule will add an average of 1 hour to an onsite inspection. We believe this is possible under the existing framework for facility and OCS facility inspections.

The Coast Guard also received an internal comment from Coast Guard District 9 that stated that we used the incorrect vessel inspector rank and wage in our analysis of Government costs.

In the NPRM, the Coast Guard assumed that vessel inspections are performed by an E–5 rank Petty Officer Second Class with a mean hourly wage rate of $58. We now assume that vessel inspections are performed by an O–2 rank Lieutenant Junior Grade with a mean hourly wage rate of $72 based on the commenter's suggestion. Readers can view the *Government Costs* section of the RA for more detail on the way this impacts the cost estimates of this final rule.

VI. Discussion of the Final Rule

This final rule adds minimum cybersecurity requirements to 33 CFR part 101 in new subpart F. Subpart F—Cybersecurity consists 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
- 101.670 Severability

A section-by-section explanation of the additions and changes follows. In addition to the additions and changes described there, we also made revisions to refer to ''U.S.-flagged vessels, facilities, and OCS facilities'' throughout for consistency and clarity related to the applicability of this final rule, as well as making other minor editorial changes.

Section 101.600—Purpose

This section states that the purpose of 33 CFR part 101, subpart F, is to set minimum cybersecurity requirements for U.S.-flagged vessels, facilities, and OCS facilities to safeguard and ensure the security and resilience of the MTS. The requirements will 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 requires that subpart F apply to the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under parts 104, 105, and 106. A list of the vessels subject to subpart F is as follows:

- U.S. mobile offshore drilling units (MODUs), cargo vessels, or passenger vessels subject to 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 rule does not apply to any foreign-flagged vessels subject to 33 CFR part 104. Cybersecurity regulations for foreign-flagged vessels under domestic law may create unintended consequences with the ongoing and future efforts to address maritime cybersecurity in the international arena and could be contrary to international law as U.S. regulatory authority over foreign-flagged vessels is limited. The traditional means to regulate vessels on the international-level is through diplomatic engagement at the IMO and through various treaty-based mechanisms. 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 and provide guidance to other flag administrations on how to regulate vessels subject to their jurisdiction.

In addition, the Coast Guard verifies how CRM is incorporated into a vessel's SMS via the process described in the updated October 11, 2023, CVC–WI–027(3), *Vessel Cyber Risk Management Work Instruction*.[62] This process will continue to be the Coast Guard's primary means of ensuring cybersecurity readiness on foreign-flagged vessels, which are exempt from this final rule. This includes working

[62] See footnote 13.

with their flag administrations to address possible deficiencies in cybersecurity.

Section 101.610—Federalism

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

Section 101.615—Definitions

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

The Coast Guard consulted several guides and authoritative sources for these new definitions. These sources include Executive Order 14028, 6 U.S.C. 148, and the Act.[63]

Another informal source for cybersecurity information is the CISA's National Initiative for Cybersecurity Careers and Studies website,[64] which is an online Federal resource for cybersecurity training and education. The Coast Guard also reviewed NIST's CSRC.[65] NIST maintains the CSRC to educate the public on computer security, cybersecurity, information security, and privacy. CISA and NIST are regarded as authoritative sources of information in areas related to technology and cybersecurity.

In addition, the Coast Guard has defined the term *cybersecurity risk* consistent with the definition at section 2200 of the Homeland Security Act of 2002 (Pub. L. 107–296), as amended. The Coast Guard notes, however, that it does not believe paragraph (7)(B) of section 2200, 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 U.S.-flagged vessels, facilities, and OCS facilities, that are the subject of this rulemaking. Therefore, we expect that exception will not be applicable to the regulated entities of this final rule. Nevertheless, for consistency with the definition found in the Homeland Security Act of 2002 and the sake of completeness, we have included the complete definition in this rule. *See also* 46 U.S.C. 70101(2); Public Law 115–254, sec. 1805(b)(2).

The Coast Guard has included definitions for *Cyber incident, Cyber risk, Cyber threat,* and *Cybersecurity vulnerability. Cyber incident* is related to *information systems* and is inclusive of both *Information Technology or IT* and *Operational Technology or OT.* The Coast Guard also defines new terms that are applicable to maritime cybersecurity, including *Critical Information Technology (IT) or Operational Technology (OT) systems, Cyber Incident Response Plan, Cybersecurity Officer or CySO,* and *Cybersecurity Plan.* A CySO, for example, is the person(s) responsible for developing, implementing, and maintaining cybersecurity portions of the VSP, FSP, or OCS FSP. The CySO also acts as a liaison with the COTP and CSOs, VSOs, and FSOs.

The Coast Guard revised some definitions to clarify their meaning based on public comments we received and added two definitions. These revisions are discussed in more detail in section V. Discussion of Comments and Changes, in the portion on *Comments Related to Definitions* in this preamble.

We revised *backup* to remove the reference to a secondary location and instead specify that the files and databases should be stored separately for preservation and recovery.

We revised *Cybersecurity Officer, or CySO* to add that owner or operator may designate an alternate CySO to assist with the duties and responsibilities of the CySO, including during periods when the CySO is on leave, unavailable, or unable to perform their duties.

We revised *Cybersecurity Plan* to add that a separate document may be submitted, in addition the originally proposed options to include the Cybersecurity Plan in the VSP, FSP, OCS FSP or the Annex to one of those plans.

We added a new definition for *log,* which means a record of the events occurring within an organization's systems and networks.

We revised *multifactor authentication* to mean more than one distinct authentication factor for successful authentication. In addition, we clarified that multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. In addition, the three authentication factors are (1) something you know, (2) something you have, and (3) something you are.

Based on support from public comments, we added a definition for *reportable cyber incident.* The definition of a *reportable cyber incident* is based on the model definition in DHS's CIRC-informed Report to Congress of September 19, 2023.[66] The term *reportable cyber incident* replaces *cyber incident* in §§ 101.620(b)(7) and 101.650(g)(1). Specifically, a reportable cyber incident means an incident that leads to, or, if still under investigation, can 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 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 final rule is to establish a threshold between the cyber incidents that have to be reported and the ones that do not.

Section 101.620—Owner or Operator

This section requires 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 that 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 include:

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

[63] Public Law 117–263, Sec. 11224(a)(1) (2022).

[64] 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 August 13, 2024.

[65] CSRC, *https://csrc.nist.gov/glossary,* accessed September 15, 2023.

[66] *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 August 13, 2024.

• Ensuring that a Cybersecurity Assessment is conducted annually or sooner, under the circumstances described in this final rule (see §§ 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 §§ 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 § 101.620(b)(5)); and

Reporting all reportable cyber incidents, including TSIs, to the NRC and relevant authorities according to the Cybersecurity Plan (see §§ 101.305 and 101.620(b)(7)). We revised this paragraph in this final rule to specify that *reportable cyber incidents* need to be reported, not all *cyber incidents.* We also removed the reference to a telephone number to allow flexibility in the way reports are made to the NRC.

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 U.S.-flagged vessel, facility, or OCS facility. The CySO needs 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 performs include ensuring development, implementation, and finalization of a Cybersecurity Plan; auditing and updating the Plan; ensuring the Cyber Incident Response Plan is executed and exercised; ensuring adequate training of personnel; and ensuring that 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 has the authority to assign cybersecurity duties to other personnel; however, the CySO remains responsible for the performance of these duties. Depending on operational conditions and cybersecurity risks, the CySO, owner, or operator may develop the required Cyber Incident Response Plan as a separate document or as an addition to the Cybersecurity Plan.

We revised § 101.625(a) to add that the CySO may serve in other roles or positions within the owner or operator's organization. In § 101.625(d)(6), we revised the text to clarify that cybersecurity inspections may be conducted in conjunction with any scheduled U.S.-flagged vessel, facility or OCS facility inspections. In § 101.625(d)(8), to allow greater flexibility for the CySO we changed the word ''ensure'' to ''enhance'' cybersecurity awareness and vigilance of personnel and removed ''through briefings, drills, exercises, and training.'' In § 101.625(d)(10), which requires the CySO to report and report information to the owner and operator, we replaced ''breaches of security, suspicious activity that may result in TSIs, TSIs, and cyber incidents'' with *reportable cyber incidents.* In § 101.625(d)(13), which covers submission of Cybersecurity Plans for approval, we removed reference to ''substantive changes (or major amendments)'' and instead only refer to amendments. In § 101.625(e) we added that a CySO may obtain the necessary qualifications for the position through education.

Section 101.630—Cybersecurity Plan

This section contains minimum requirements for the Cybersecurity Plan. The Cybersecurity Plan must 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* § 101.640. A Cybersecurity Plan incorporates the results of a Cybersecurity Assessment and considers the recommended measures appropriate for the U.S.-flagged vessel, facility, or OCS facility. A Cybersecurity Plan can be combined with or complement an existing FSP, VSP, or OCS FSP. We revised § 101.630(a) to add that a separate submission may be used in addition to the originally proposed options to include the Cybersecurity Plan in the VSP, FSP, OCS FSP or the Annex to one of those Plans.

A Cybersecurity Plan can 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 final rule includes the following individual sections:

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

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

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

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

(5) Communications (see § 101.645 Communications);

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

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

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

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

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

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

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

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

Depending on operational conditions and cybersecurity risks, the owner or operator may develop the required 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 must submit a Cybersecurity Plan for review to the cognizant COTP or the OCMI for facilities and OCS facilities, or to the MSC for U.S.-flagged vessels. *See* § 101.630(d). We removed the requirement for a letter certifying that the Plan meets the requirements of this subpart must accompany the submission in § 101.630(d). Once the COTP or MSC finds that the Plan meets the cybersecurity requirements in

§ 101.630, they will 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 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* § 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 will be returned to the owner or operator with a letter explaining why the Plan did not meet the requirements. In this final rule, we revised § 101.630(e)(1)(ii) to clarify that the owner or operator has at least 60 days to submit its proposed amendments. Until the amendments are approved, the owner or operator must ensure temporary cybersecurity measures are implemented to the satisfaction of the Coast Guard. *See* § 101.630(e)(1)(ii).

If the owner or operator disagrees with the deficiency determination, they have the right to appeal or submit a petition for reconsideration or review to the respective COTP, District Commander, OCMI, or MSC per 33 CFR 101.420.

When submitting amendments to the Coast Guard, either after a Cybersecurity Assessment or at other times, the owner or operator is not required to submit the Cybersecurity Plan with the amendment. Consistent with the discussion above concerning our elimination of the term ''major amendment,'' we removed the reference to major amendment from § 101.630(e)(2). We added a new paragraph, § 101.630(e)(2)(i), which provides that nothing in this section should be construed as limiting the owner or operator of the U.S.-flagged vessel, facility, or OCS facility from the timely implementation of such additional security measures not enumerated in the approved VSP, FSP, or OCS FSP as necessary to address exigent security situations. This new paragraph addresses questions from public commenters about whether entities would be able to implement necessary changes to their Plan to protect against cybersecurity threats and clarifies that stakeholders are not precluded from taking action to protect their systems.

Additionally, we moved the requirement that the owner or operator must notify the cognizant COTP for a facility or OCS facility, or the MSC for U.S.-flagged vessels, by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place into new paragraph § 101.630(e)(2)(ii). This paragraph provides that when the entity makes changes that do not allow for Coast Guard approval before implementation, they must notify the appropriate Coast Guard contact as soon as possible so that the Coast Guard has the most up-to-date and accurate description of the Cybersecurity Plan.

Finally, we clarified in § 101.630(e)(3) and (4) that the CySO must amend the Cybersecurity Plan, as soon as reasonably practicable, in light of the individual circumstances, but, in any case, not longer than 96 hours, when the owner or operator has changed.

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 must 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 § 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 amendments to the Coast Guard for review within 30 days of completing the audit.

Section 101.635—Drills and Exercises

Under § 101.635(a)(1), cybersecurity drills and exercises are 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 must also enable the CySO to identify any related cybersecurity deficiencies that need to be addressed. Additionally, in § 101.635(a)(2), we changed ''cyber incident'' to a ''reportable cyber incident.''

Cybersecurity drills 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. In this final rule, we changed the requirement in § 101.635(b)(1) from conducting at least one cybersecurity drill every 3 months to conducting two cybersecurity drills every 12 months, and added ''as required by 33 CFR 104.230, 105.220, or 106.225,'' where appropriate.

Cybersecurity exercises are a full test of an organization's cybersecurity regime and include substantial and active participation of cybersecurity personnel. The participants may include local, State, and Federal Government personnel. Cybersecurity exercises 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 are required at least once each calendar year, with no more than 18 months between exercises. In § 101.635(c)(2)(iii), where exercises may be combined with other appropriate exercises, we added ''as required by 33 CFR 104.230, 105.220, or 106.225.'' Exercises may be specific to a U.S.-flagged vessel, facility, or OCS facility, or may serve as part of a cooperative exercise program or port exercises. The exercises for the Cybersecurity Plans can be combined with other required security exercises, if appropriate.

The 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 U.S.-flagged 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 section requires 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 U.S.-flagged vessel, facility, or OCS facility keep vary because each organization maintains records specific to their operations. At a minimum, the records must capture the following activities: training, drills, exercises, cybersecurity threats, reportable cyber 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. We revised the list of activities in § 101.640 to replace ''incidents'' with ''reportable cyber incidents,'' since we have revised this final rule to use that term.

Section 101.645—Communications

This section requires 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 must 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. We revised § 101.645(a) to clarify that the means for effective notification must be documented in Section 5 of the Cybersecurity Plan. Documenting the communication process for changes will promote active information sharing among the various people responsible for the cybersecurity measures of the U.S.-flagged vessel, facility, or OCS facility.

Section 101.650—Cybersecurity Measures

This section lists specific cybersecurity measures to identify risks, detect threats and vulnerabilities, protect critical systems, and recover from cyber incidents. Any intentional gaps in cybersecurity measures must be documented as accepted risks under § 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 § 101.665.

A discussion of each component of § 101.650 follows.

Section 101.650 Paragraph (a): Account Security Measures

This paragraph lists 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, highlighted as a ''Protect'' function of NIST's CSF.[67] 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, facilities, OCS facilities, or ports. This provision is 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.

Account security measures for cybersecurity 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.[68] Together, these provisions mitigate the risks of brute force attacks, unauthorized access, and privilege escalation. The owner or operator is 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 must ensure documentation of such measures in Section 7 of the Cybersecurity Plan. We revised § 101.650(a)(1), which required automatic account lockouts after repeated failed login attempts for both IT and OT systems to remove the reference to OT systems. In § 101.650(a)(2), we added the information that, when changing default passwords is not feasible, appropriate compensating security controls must be implemented and documented.

Section 101.650 Paragraph (b): Device Security Measures

This paragraph provides specific 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, facilities, and OCS facilities have an expansive attack surface. These provisions reduce the risks of unauthorized access, malware introduction, and service interruption. This paragraph applies the ''Identify'' function of the NIST CSF.[69] 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.

Paragraph (b) also requires owners and operators to designate critical IT and OT systems.[70] Developing and maintaining an accurate inventory and network map reduces the risk of unknown or improperly managed assets. The Cybersecurity Plan also governs device management. The CySO must maintain the network map and develop and maintain the list of approved hardware, software, and firmware. In addition to identifying risks, these provisions 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 reinforce Coast Guard regulations to protect communication networks. We revised § 101.650(b) to require that device security measures must be addressed, rather than documented, in Section 6 of the Cybersecurity Plan and also to clarify that they must be made available to the Coast Guard upon request. In § 101.650(b)(2), we removed the requirement that exemptions must be justified and documented in the Cybersecurity Plan.

Section 101.650 Paragraph (c): Data Security Measures

This paragraph prescribes 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,[71] and the Coast Guard previously highlighted data security

[67] NIST CSF, *www.nist.gov/cyberframework/protect,* accessed August 13, 2024.

[68] *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.

[69] NIST CSF; Identify, ''NIST Cybersecurity Publication by Category,'' *Asset Management ID.AM,* updated May 3, 2021, *www.nist.gov/cyberframework/identify,* accessed August 13, 2024. 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 13, 2024.

[70] To help CySOs identify which systems are critical, 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 August 13, 2024, 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 August 13, 2024.

[71] 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.''

measures in its policy for MTSA-regulated facilities.[72]

Data security measures prevent data loss and aid in detection of malicious activity on critical IT and OT systems. The fundamental measures here establish baseline protections upon which owners and operators can build. This paragraph requires logs to be securely captured, stored, and protected so that they are accessible only by privileged users, and require encryption for data in transit and data at rest. CySOs will 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. [73] Consistent with the discussion earlier about the term ''logs,'' we revised § 101.650(c)(1) to refer to logs, which we have defined in this final rule, rather than data logs. Additionally, we revised § 101.650(c)(2) to provide that effective encryption must be deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic, when technically feasible, rather than specifically referring to suitably strong algorithms. A CySO must establish detailed data security policies in Section 4 of the Cybersecurity Plan, adapting these policies 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 specifies 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.'' [74] Since 2020, the Coast Guard has interpreted this requirement to include relevant cybersecurity training.[75] While formal training may be appropriate, the Coast Guard is not mandating a format of training. However, the training must, at minimum, cover relevant provisions of the Cybersecurity Plan to include recognizing, detecting, and circumventing cybersecurity threats; and reporting cyber incidents to the CySO.

The types of training must also 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 need to have current knowledge of threats to deal with potential cyber-attacks and understand procedures for responding to a cyber incident. The owner, operator, or CySO must ensure that 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 are 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 this final rule and annually thereafter. (See § 101.650(d)(4)). We added a requirement in § 101.650(d)(3) that when personnel must access IT or OT systems but are unable to receive cybersecurity training as specified in paragraphs (d)(1) and (d)(2) of this section, they must be accompanied or monitored by a person who has completed the training specified in paragraphs (d)(1) and (d)(2) of this section. As a result, we redesignated the originally proposed § 101.650(d)(3) as § 101.650(d)(4).

Section 101.650 Pharagraph (e): Risk Management

This paragraph establishes 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 owner, operator, or designated CySO must 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 must incorporate feedback from the assessment into the Cybersecurity Plan through an amendment to the Plan. We revised the timeframe that a Cybersecurity Assessment must be conducted from within 1 year from the effective date of a final rule and annually thereafter to 24 months after the effective date of the final rule and annually thereafter. The Assessment must be conducted sooner than annually if there is a change in ownership of a U.S.-flagged vessel, facility, or OCS facility. We removed the requirement for more frequent Cybersecurity Assessments if there is a major amendment to the Cybersecurity Plan.

We updated the implementation period in § 101.650(e)(1) to be 24 months from the effective date of this final rule. We revised § 101.650(e)(1)(i) to clarify that owners or operators must analyze all networks to identify vulnerabilities to *critical* IT and OT systems and the risk posed by each digital asset. We added a new paragraph § 101.650(e)(1)(iv) to explain that the Cybersecurity Assessment must document and ensure patching or implementing of documented compensating controls for all KEVs in critical IT or OT systems, without delay, rather than mitigate any unresolved vulnerabilities. We also redesignated the originally proposed § 101.650(e)(1)(iv) as § 101.650(e)(1)(v).

While Cybersecurity Assessments provide a valuable picture of potential security weaknesses, penetration tests can add additional context by demonstrating whether malicious actors can leverage those weaknesses. Penetration tests can also help prioritize resources based on what poses the most risk. We revised § 101.650(e)(2) to specify that penetration testing must be conducted in conjunction with Plan renewal and that a letter certifying that the test was conducted, as well as all identified vulnerabilities, must be included in the VSA, FSA, or OCS FSA.

Routine system maintenance requires an ongoing effort to identify vulnerabilities and must include scanning and reviewing KEVs by documenting, tracking, and monitoring them. These provisions 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, each owner, operator, or designated CySOs must establish, subject to any applicable antitrust law limitations,[76] information-sharing

[72] 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 . . . . ''

[73] *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 August 13, 2024.

[74] 33 CFR 104.225(c) (Vessels), 105.215(c) (Facilities), and 106.220(c) (OCS Facilities).

[75] 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.''

[76] 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,

procedures for their organizations, to 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.[77] For example, organizations must ensure that 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 does not endorse specific information-sharing organizations; owners and operators are free to use information-sharing organizations to suit their needs.[78] Industry consensus standards provide generally accepted techniques that sanitize and reduce attribution to information to ensure that information sharing does not compromise proprietary business information.[79] In addition, regardless of the services or organizations used, owners and operators should comply with applicable antitrust laws and 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 do 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 *2023 Cyber Trends and Insights in the Marine Environment* report.[80] 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 paragraph includes 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.[81]

Under this paragraph, the owner, operator, or CySO must ensure that measures to manage cybersecurity risks in the supply chain are in place to mitigate the risks associated with external parties. These measures include considering cybersecurity capabilities in selecting vendors, establishing a process through which all IT and OT vendors or service providers notify the owner or operator or designated CySO of any cybersecurity vulnerability or reportable cyber incident, without delay, and monitoring third-party connections. In § 101.650(f)(3), we replaced ''incidents'' with ''reportable cyber incidents,'' since we have revised this final rule to use that term, where applicable, and removed ''breaches.''

Through their contractual agreements, vendors must ensure the integrity and security of software and hardware, such as software releases and updates, notifications, and mitigations of vulnerabilities. These provisions must establish a minimum level of CRM within the supply chain. Industry standards provide additional measures.[82] The IMO also recognizes cybersecurity risks in the supply chain, and these provisions align with the guidelines and recommendations referenced in MSC–FAL Circ. 3/Rev.1.[83]

Section 101.650 paragraph (g): Resilience

This paragraph lists 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 final rule requires the owner, operator, or CySO to ensure the following response and recovery activities: report reportable cyber incidents to the NRC; 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 accepts review of a cyber incident as meeting the periodic validation requirement in § 101.650(g). We revised § 101.650(g)(1) to replace the provisional ''any cyber incidents'' with ''reportable cyber incidents,'' since that is now a defined term in this final rule, after we received and considered public comments on that term. We removed the reference to a telephone number for reporting to the NRC. We also revised § 101.650(g)(3) to remove ''tabletop'' and refer only to ''exercises.'' The Coast Guard changed this for consistency with § 101.635, which defines ''exercises'' to include live exercises as well as ''tabletop simulations.'' The intent here is to use the more general ''exercises,'' which includes but is not limited to tabletop exercises or simulations, for consistency with § 101.635.

In addition, the NIST CSF describes numerous provisions within the ''Recover'' function aimed at improving response and recovery.[84] The IMO also notes resilience.[85]

Section 101.650 Paragraph (h): Network Segmentation

This paragraph requires a CySO to ensure that 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.[86] Network architectures vary widely based on the operations of a U.S.-flagged vessel, facility, or OCS facility. Separating IT and OT networks is challenging, and it

boycotting, monopolistic conduct, or other collusive conduct.

[77] 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 August 13, 2024.

[78] The Coast Guard encourages CySOs to explore resources through CGCYBER Maritime Cyber Readiness Branch, available at *https://www.uscg.mil/MaritimeCyber/,* accessed August 13, 2024*; see also* CISA's ''Information Sharing and Awareness,'' available at *https://www.cisa.gov/information-sharing-and-awareness,* accessed August 13, 2024.

[79] *See,* for example, 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 August 13, 2024.

[80] ''2023 Cyber Trends and Insights in the Marine Environment,'' April 12, 2024, *https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf,* accessed August 13, 2024.

[81] NIST CSF, Version 1.1, ''ID.SC: Supply Chain Risk Management,'' *https://csf.tools/reference/nist-cybersecurity-framework/v1-1/id/id-sc/*, accessed August 13, 2024.

[82] *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 August 13, 2024.

[83] MSC–FAL.1/Circ.3/Rev.1, 2.1.6 and 4.2; see footnote 34.

[84] NIST CSF, Version 1.1 ''RC: Recover,'' *https://csf.tools/reference/nist-cybersecurity-framework/v1-1/rc/*, accessed August 13, 2024.

[85] MSC–FAL Circ. 3/Rev. 1, 3.5.5; see footnote 34.

[86] NIST CSF, Version 1.1, ''PR.AC–5: Network integrity is protected (for example, network segregation, network segmentation).'' *csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ac/pr-ac-5/*, accessed July 19, 2023.

becomes increasingly difficult with an increase in the various devices connected to the network. Network segmentation ensures that 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.[87]

Section 101.650 Paragraph (i): Physical Security

This paragraph specifies that, along with the cybersecurity provisions for inclusion in this part, owners, operators, or CySOs must 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).[88] Physical security measures here supplement the existing 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 paragraph, the CySO must designate areas restricted to authorized personnel and secure HMIs and other hardware. Also under this paragraph, the CySO must establish policies to restrict the use of unauthorized media and hardware. These provisions mirror existing Coast Guard policy outlined in NVIC 01–20.[89]

Section 101.655—Cybersecurity Compliance Dates

This section states that a Cybersecurity Plan, as required by this final rule, must be made available to the Coast Guard for review no later than 24 months from the effective date of this final rule, as required by 33 CFR 104.410 for vessels, 33 CFR 105.410 for facilities, and 33 CFR 106.410 for OCS facilities. We updated § 101.655 to reflect the revised implementation period. We also corrected the cross-references in this section from §§ 104.415, 105.415, and 106.415 to §§ 104.410, 105.410, and 106.410, respectively.

Section 101.660—Cybersecurity Compliance Documentation

This section allows the Coast Guard to verify an approved Cybersecurity Plan for U.S.-flagged vessels, facilities, and OCS facilities. 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. We revised what we proposed in § 101.660 to expressly state that Alternative Security Program provisions apply to cybersecurity compliance documentation.

Section 101.665—Noncompliance, Waivers, and Equivalents

This section provides owners and operators the opportunity for waiver and equivalence determinations from the cybersecurity requirements in subpart F of this final rule, pursuant to the existing regulations in 33 CFR 104.130, 104.135, 105.130, 105.135, and 106.130. Under this section, an owner or operator, after completion of the required Cybersecurity Assessment, may seek a waiver or an equivalence determination for the requirements in subpart F using the standards and submission procedures applicable to a U.S.-flagged vessel, facility, or OCS facility, as outlined in 33 CFR 104.130, 104.135, 105.130, 105.135, 106.125, or 106.130.

The Coast Guard revised § 101.665 to clarify that the owner or operator must conduct the Cybersecurity Assessment prior to requesting a waiver or equivalence because it is not possible to know if a requirement is unnecessary until the Cybersecurity Assessment is completed. As previously noted, one of the primary purposes of an Assessment is to identify whether there are actual or potential vulnerabilities to IT or OT systems, equipment, or procedures. The Assessment is the evaluation that helps determine whether there exists IT or OT systems, equipment, procedures, or other cyber elements that may be applicable to these rules. It is the review a regulated entity can point to in explaining why the request for a waiver or equivalence is necessary.

The Coast Guard finds it unlikely that any regulated entity would have no IT or OT systems or equipment. However, if an entity has no IT or OT footprint, then their Assessment would easily identify that fact.

While this was implied and accounted for in the NPRM by our assumption that all owners and operators would need to complete a Cybersecurity Assessment and Plan (see RA, section *Cybersecurity Plan Costs*), we have now stated this explicitly within the text. The Coast Guard will also need the information an owner or operator will gain from completing an Assessment to assess the flexibility possible for the entity making the request, in light of their individual circumstances.

The Coast Guard removed the text requiring the vessel or facility to be ''unable to meet the requirements in subpart F,'' as originally proposed. Instead, we specify that the waiver or equivalence determination may be sought using the same standards and submission procedures applicable to a U.S.-flagged vessel, facility, or OCS facility, as outlined in 33 CFR 101.130, 104.130, 104.135, 105.130, 105.135, 106.125, or 106.130. We made this change for consistency with the existing waiver and equivalence provisions in 33 CFR parts 104, 105, and 106.

Additionally, this section provides that, if an owner or operator must temporarily deviate from the requirements in this part, they must notify the cognizant COTP for facilities or OCS facilities, or the MSC for U.S.-flagged vessels, and may request temporary permission to continue to operate under the provisions as outlined in 33 CFR 104.125, 105.125, or 106.120. We updated this text from ''if an owner or operator is temporarily unable to meet'' the requirements to ''if an owner or operator must temporarily deviate from'' for consistency with existing temporary waiver regulations as outlined in 33 CFR 104.125, 105.125, or 106.120.

Finally, the Coast Guard made editorial changes within § 101.665 to reflect that facilities and OCS facilities will notify the cognizant COTP for temporary waiver requests, whereas U.S.-flagged vessels will make this notification to the MSC.

Section 101.670—Severability

This section reflects the Coast Guard's intent that the provisions of subpart F be considered severable from each other to the greatest extent possible. For instance, if a court of competent jurisdiction were to hold that this final rule or a portion thereof may not be applied to a particular owner or operator or in a particular circumstance, the Coast Guard intends for the court to leave the remainder of this final rule in place with respect to all other covered persons and circumstances. The inclusion of a severability clause in subpart F does not imply a position on

[87] *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.

[88] 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.

[89] 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).

severability in other Coast Guard regulations.

Section 160.202—Definitions

This section revises the definition for hazardous condition to add cyber incident. In the NPRM, we requested public comments on whether we should amend this definition, and commenters were supportive of the change, as discussed previously.

VII. Request for Comment

The Coast Guard requests public comment on a potential 2-to-5-year delay for the implementation periods for new requirements applicable to U.S.-flagged vessels. This rule contains three broad categories of implementation periods, only two of which would be affected by a delay.

First, entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16–1 must ensure that all reportable cyber incidents are reported to the NRC (§ 101.620(b)(7)) immediately upon the effective date of this rule. Because U.S.-flagged vessels have been subject to the reporting requirements in 33 CFR 6.16–1 since the issuance of Executive Order 14116 on February 21, 2024, we are not seeking comments on whether to delay the implementation period for incident reporting.

Second, this rule contains a variety of training requirements in § 101.650 that must be implemented within 6 months after the effective date of this rule.

Third, this rule contains three provisions, as follows, that must be implemented within 24 months after the effective date of this rule:

- Owners and operators must designate, in writing, the CySO (§ 101.620(b)(3) and (c)(1));
- Owners and operators must conduct the Cybersecurity Assessment within 24 months after the effective date of this final rule and annually thereafter (or sooner than annually if there is a change in ownership) (§ 101.650(e)(1)); and
- Owners and operators must submit the Cybersecurity Plan to the Coast Guard for approval within 24 months after the effective date of this final rule (§ 101.655).

As noted in Section V of this preamble, the Coast Guard received several public comments asking us to extend the implementation period for different periods, ranging from 36 to 48 months beyond those we proposed in the NPRM. Many of these comments were specific to vessels. Some commenters suggested that U.S.-flagged vessels would require more time than facilities to implement new requirements in this rule because of differences in the pre-existing guidance provided for vessels in CVC–WI–027(3), Vessel Cyber Risk Management Work Instruction, as opposed to guidance for facilities in NVIC 01–20, Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities.[90] Some commenters also remarked on the rule's potential burden on U.S.-flagged vessels, writing that the United States should not impose specific requirements for the flag state on its vessels without imposing the same on foreign-flagged vessels. A commenter asserted that, once the IMO establishes international requirements, a new NPRM should be issued to implement these requirements for U.S.-flagged vessels. And some commenters remarked upon U.S.-flagged vessels' ability to complete training requirements within six months of the rule's effective date.

As described earlier in this preamble, in response to these comments, the Coast Guard has adjusted the final rule generally to contain a phased-in implementation schedule that results in greater lead time for implementation. Particularly in light of the public comments specific to vessels described in the previous paragraph, the Coast Guard invites the public to comment on whether we should further delay the implementation periods for new requirements applicable to U.S.-flagged vessels for a period of 2 to 5 years beyond what is specified in this rule. Comments submitted should include information supporting the specific period that the commenter suggests, with respect to specific provisions of the rule. (See the **ADDRESSES** portion of this preamble, under *Comment period for solicited additional comments,* for instructions on submitting comments.) After reviewing any comments and supporting information received, the Coast Guard may issue a future rule to implement this additional delay to provide time for U.S.-flagged vessels to come into compliance with these requirements. The Coast Guard also welcomes comment on whether a delay for vessels alone could result in unanticipated consequences for facilities.

VIII. Regulatory Analyses

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

[90] See footnote 13.

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.

The Office of Management and Budget (OMB) has designated this rule a ''significant regulatory action,'' as defined 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 rule. A final RA follows.

The Coast Guard received 99 comment submissions during the 90-day comment period that ended on May 22, 2024. We received numerous public comments related to the RA in the NPRM, including several commenters stating that the Coast Guard underestimated the costs related to certain provisions. These provisions included supply chain measures, device security measures, penetration testing, routine system maintenance, drills and exercises, network segmentation, CySO wages, and OCS facility inspections. In light of some of these comments, we have increased certain cost estimates associated with drills, exercises, and penetration testing. In addition, we have lowered the proposed frequency of drill requirements from quarterly to twice annually, which reduces the real burden faced by affected entities, even though our increased hour burden estimates associated with development and participation involved with drill and exercise requirements have increased our cost estimates. This also increases marginal benefits of drills by allowing owners and operators to develop and focus on more comprehensive drills for the remaining drills or allocate resources to the implementation or improvement of other cybersecurity measures. Beyond these cost estimate updates, and an update to our affected population based on a discrepancy noted by another public commenter, the

methodology employed in the RA is unchanged.

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 final rule.

Agency/Program Office: U.S. Coast Guard

Rule Title: Cybersecurity in the Marine Transportation System

RIN#: 1625–AC77

Date: August 2024 (millions, 2022 dollars)

Table 2: OMB Circular A-4 Accounting Statement Categorizing Impacts for the Cybersecurity in the Marine Transportation System Final Rule

Category	*Primary Estimate*	*Low Estimate*	*High Estimate*	*Dollar Year*	*Discount Rate*	*Time Horizon*	*Source*
BENEFITS							
Annualized monetized benefits	-	-	-	2022	2%	10 Years	RA
Annualized quantified, but non-monetized, benefits	-	-	-	2022	2%	10 Years	RA
	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 data of MTS firms and customers to safeguard business operations, build consumer trust, and promote increased commerce in the U.S. economy.						RA
Unquantified benefits	Improve the minimum standard for cybersecurity to protect the MTS and avoid disruptions to the supply chain, which is vital to the U.S. economy and U.S. national security.						RA
COSTS							
Annualized monetized costs	$138.7 million	-	-	2022	2%	10 Years	RA
Annualized quantified, but non-monetized, costs	-	-	-	2022	2%	10 Years	RA
Unquantified costs	The unquantifiable costs of this final rule are associated with the actions to mitigate the cyber risks identified as a result of this final rule. 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 final rule.						RA
TRANSFERS							
Annualized monetized Federal budgetary transfers	N/A	N/A	N/A				
Bearers of transfer gain and loss?	N/A	N/A	N/A				
Other annualized monetized transfers	N/A	N/A	N/A				
Bearers of transfer gain and loss?	N/A	N/A	N/A				
NET BENEFITS							
Annualized monetized net benefits	-	-	-				
Effects on State, local, or Tribal governments	None						

Effects on small businesses	We conducted a FRFA and estimate that this final rule will have a significant economic impact on a substantial number of small entities.	RA/FRFA
Effects on wages	None	
Effects on growth	Not measured	

The Coast Guard has updated its maritime security regulations by adding minimum cybersecurity requirements to a new subpart F in 33 CFR part 101 for U.S.-flagged vessels, facilities, and OCS facilities required to have a security plan under 33 CFR parts 104, 105, and 106. Specifically, this final rule requires owners and 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 includes the following: 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 final rule further requires owners and operators of U.S.-flagged vessels, 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 are also required to maintain records of cybersecurity related information in paper or electronic format.

Lastly, this final rule requires 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 final rule. The requirements of this final rule and the costs and benefits we estimate in this RA are new. The Coast Guard drafted the requirements of this final 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 to 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 7 years. In 2017, the IMO adopted resolution MSC.428(98) to the ISM Code on ''Maritime Cyber Risk Management in Safety Management Systems.'' 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 awareness about cybersecurity risks in the maritime domain.

In addition, survey data indicates that some portions of the affected population of owners and operators of facilities and OCS facilities are already implementing cybersecurity measures consistent with select provisions of this final 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.[91] 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 purpose 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 this Final Rule

We estimate the total discounted costs of this final rule to industry and the Federal Government to be approximately $1,245,594,930 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $138,667,759, using a 2-percent discount rate. See table 3.

[91] See footnote 60. In addition, for our cybersecurity training assumption, we use the more conservative brown-water facility rate of 25 percent rather than the blue-water rate of 57 percent given a lack of data about which facilities in the affected population would be considered brown- or blue-water. Further, while the survey does not specify if any of the surveyed population includes OCS facilities, the Coast Guard assumes that findings reflect current compliance for OCS facilities because we assume the scale of port and terminal operations surveyed would be similar to those on the OCS. Readers can access the survey at *https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html,* accessed August 26, 2024.

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

Year	Facility and OCS Facility Costs	U.S.-flagged Vessel Costs	Government Costs	Total Costs	2 Percent
1	$57,844,636	$81,181,976	$402,629	$139,429,241	$136,695,334
2	$68,199,840	$110,518,021	$18,794,061	$197,511,922	$189,842,293
3	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$118,315,883
4	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$115,995,964
5	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$113,721,533
6	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$111,491,699
7	$55,920,448	$105,034,449	$4,809,252	$165,764,149	$144,307,667
8	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$107,162,341
9	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$105,061,119
10	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$103,001,097
Total	**$572,198,376**	**$768,567,346**	**$40,843,924**	**$1,381,609,646**	**$1,245,594,930**
Annualized					**$138,667,759**

Note: Totals may not sum due to independent rounding.

We present a summary of the impacts of this final rule in table 4.

Table 4: Summary of Impacts of the Final Rule

Category	Summary
Applicability: 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 1,372 facility owners and operators of approximately 3,718 facilities (33 of which are OCS facilities, with 9 unique owners or operators). • Approximately 2,075 U.S.-flagged vessel owners and operators of approximately 11,222 U.S.-flagged vessels (or 1,686 owners and operators of 6,379 U.S.-flagged vessels, excluding barges, where applicable).
Total Costs of the Final Rule (2-percent discount rate—all estimates in table)	**Costs to Industry:** Total discounted cost: $1.2 billion Annualized cost: $134.5 million Total discounted cost to facilities and OCS facilities cost $514.9 million Annualized cost: $57.3 million Total discounted cost to only OCS facilities: $3.7 million Annualized cost: $0.4 million Total discounted cost to U.S.-flagged vessels: $693.2 million Annualized cost: $77.2 million **Costs to Federal Government:** Total discounted cost: $37.5 million Annualized cost: $4.2 million **Total Costs of Final Rule:** Total discounted cost: $1.2 billion Annualized cost: $138.7 million

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 logs and backups. • Costs associated with disabling applications running executable code. • Costs associated with monitoring and all remote third-party connections. • Costs associated with patching and scanning for vulnerabilities in OT systems. • 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 this final 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.

Public Comments and Changes From the NPRM to the Final Rule

The Coast Guard received numerous public comments with implications for the RA. Summaries of those comments, and the Coast Guard's responses, are found in section V., Discussion of Comments and Changes, in the preamble of this final rule.

Table 5 describes the resulting changes from comments and the impacts on our cost estimates for this final rule. In addition to the changes described in table 5, the Coast Guard has also updated the analysis to a 2-percent discount rate, consistent with guidance in the updated OMB Circular A–4, published November 2023.[92]

[92] See page 75 in OMB Circular A–4, Regulatory Analysis, found at: *https://www.whitehouse.gov/wp-content/uploads/2023/11/CircularA-4.pdf,* accessed August 26, 2024.

Table 5: Summary of Changes from NPRM to Final Rule

Element of the Analysis	NPRM	Final Rule	Resulting Change in the RA[93]
Affected Population	10,286 U.S.-flagged vessels (1,775 owners and operators) and 3,411 facilities and OCS facilities (1,708 owners and operators). Inadvertently excluded a portion of publicly owned vessels and facilities from the affected population.	11,222 U.S.-flagged vessels (2,075 owners and operators) and 3,718 facilities and OCS facilities (1,372 owner and operators). Now includes impacted publicly owned vessels and facilities and more accurately consolidates the number of owners and operators.[94]	-Increases total and annualized cost estimates for the rule. NPRM Costs (2%): Total cost - $711.7M Annualized - $79.2M Final Rule Costs (2%): Total cost - $1.2B Annualized - $138.7M
Cybersecurity Drills in § 101.635(b)	Cybersecurity drills required every 3 months or quarterly combined with existing physical security drills required under 33 CFR parts 104, 105, and 106. Cost estimates based on the CySO developing cyber components to add to existing drills, taking 30 minutes per drill, or 2 hours annually.	Cybersecurity drills required twice annually and held separately with all employees participating. Cost estimates based on the CySO developing new cybersecurity drills, taking 8 hours per drill, or 16 hours annually. 33 percent of employees per owner or operator will take 4 hours to participate in each drill, or 8 hours annually.	-Halving the annual drill requirement lowers the burden on the affected population, but the total and annual cost estimates for drills are increased. NPRM Costs (2%): Total cost - $5.3M Annualized - $0.6M Final Rule Costs (2%): Total cost - $298M Annualized - $33.2M
Cybersecurity Exercises in § 101.635(c)	Cybersecurity exercises required annually combined with existing physical security exercises. Cost estimates based on the CySO developing cyber components to add to existing exercises, taking 8 hours annually.	Cost estimates based on the CySO developing cyber exercises, taking 20 hours annually, and participating employees taking 4 hours annually. 33 percent of employees estimated to participate in cybersecurity exercises.	-Increased total and annualized exercise cost estimates. NPRM costs (2%): Total cost - $21.1M Annualized - $2.3M Final Rule costs (2%): Total cost - $180.3M Annualized - $20.1M
Penetration Testing in § 101.650(e)(2)	Testing required with submission of the Cybersecurity Plan in Years 2 and 7 of the period of analysis.	Initial cost estimate increased to $10,000 and $100 per IP address. Number of employees multiplied	- Increased total and annualized penetration testing cost estimates. NPRM costs (2%):

	Initial cost estimate was $5,000 for a third party to conduct the test, and $50 per IP address. Number of employees used as a proxy for number of IP addresses at a given company.	by 2 used as a proxy for the number of IP addresses at a given company.	Total cost - $35M Annualized - $3.9M Final Rule costs (2%): Total cost - $100.2M Annualized - $11.2M
Vessel Inspector Wage	Vessel inspector assumed to be an E-5 rank Petty Officer Second Class with a mean hourly wage rate of $58.	Vessel inspector assumed to be an O-2 rank Lieutenant Junior Grade with a mean hourly wage rate of $72.	- Increased total and annualized Government vessel inspection cost estimates. NPRM costs (2%): Total cost - $894,935 Annualized - $0.1M Final rule costs (2%): Total cost - $1.2 million Annualized - $0.1M
Reportable Cyber Incident Reporting	20 reportable cyber incidents required to be reported to NRC annually (18 from facilities population, and 2 from vessel population). Estimated that each incident took 0.15 hours to report.	Reportable cyber incidents only required to be reported to NRC for the population of 33 OCS facilities not already required to report cyber incidents under 33 CFR 6.16-1, as amended by Executive Order 14116. With only 1 reportable cyber incident report by OCS facilities since 2018, we consider the annual estimated costs negligible in the final rule.	- Removes total and annualized reportable cyber incident reporting costs. NPRM Costs (2%): Total cost - $2,263 Annualized - $252 Final rule costs (2%): Total cost - $0 Annualized - $0

Affected Population

This final rule affects 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 final rule will affect approximately 11,222 vessels and 3,718 facilities (including 33 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;
- 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

[93] We have updated NPRM cost totals to 2-percent discounting to better compare with the estimated cost totals from the final rule.

[94] See table 6 for more information on the number of affected facilities and OCS facilities and U.S.-flagged vessels by vessel type. Along with changes related to the inclusion of publicly owned vessels, removal of duplicate vessels in the Sub I vessel population, and more accurately consolidating the counts of owners and operators, the number of towing vessels has increased by approximately 901 vessels (4,822–3,921 = 901) primarily due to the ''Inspection of Towing Vessels'' final rule published June 20, 2016. See 81 FR 40004 or 46 CFR 136.202(a). This final rule requires owners and operators owning more than 1 towing vessel to have 100 percent of their towing vessels inspected and have valid certificates of inspection by July 19, 2022. This means our original data missed some of the affected population of towing vessels because their inspections were not yet recorded in MISLE when we pulled our data for the NPRM.

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 6 presents the affected population of U.S.-flagged vessels, facilities, and OCS facilities of this final rule.[95] 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 is very rare, and any audits that result from a change in ownership are accounted for by the annual audit requirements.

[95] This data was retrieved from the Coast Guard's MISLE database in July 2024.

Table 6: Estimated Affected U.S. Population of the Final 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.	4,822
U.S. tankships inspected under 46 CFR subchapters D and O.	114
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.	398
Small U.S. passenger vessels carrying more than 12 passengers, including at least 1 passenger-for-hire, that are engaged on international voyages.	53
Small U.S. passenger vessels inspected under 46 CFR subchapter K (certificated to carry more than 150 passengers).	430
Large U.S. passenger vessels inspected under 46 CFR subchapter H.	131
OSVs inspected under 46 CFR subchapter L	430
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.	4,843
Total U.S.-flagged vessel population	**11,222 (2,075 owners and operators)**
Facilities	
33 CFR part 105 - facilities	**3,685**
33 CFR part 106 - OCS facilities	**33**
Total facilities and OCS facilities (includes MTSA-regulated facilities)	**3,718 facilities (1,372 owners and operators)**

Cost Analysis of the Final Rule

This final rule imposes costs on the U.S. maritime industry for cybersecurity requirements that include:

- Developing a Cybersecurity Plan, which includes designating a CySO, in 33 CFR 101.630;
- Performing drills and exercises in 33 CFR 101.635; and
- Ensuring and implementing cybersecurity measures in 33 CFR 101.650, such as account security measures, device security measures, data security measures, cybersecurity

training for personnel, reporting cyber incidents, 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.

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 final rule, in most cases, barges do not have IT or OT systems on board. Many types of barges rely on the IT and OT systems on board 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 on board, 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 do not apply to a vessel or vessel company lacking significant IT or OT systems.

Cybersecurity Plan Costs

Each owner and operator of a U.S.-flagged vessel, facility, or OCS facility is required to develop and submit a Cybersecurity Plan to the Coast Guard. The CySO will develop, implement, and verify a Cybersecurity Plan for each U.S.-flagged vessel, facility, or OCS facility. The owner or operator will submit a copy of 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 § 101.630.

Unless otherwise stated, in this RA we used information and obtained estimates from SMEs in the Coast Guard's Office of Commercial Vessel Compliance (CG–CVC), CG–FAC, and the Coast Guard's Office of Design and Engineering Standards (CG–ENG). We also obtained information from CGCYBER and NMSAC.

The Coast Guard acknowledges that some owners and operators of U.S.-flagged vessels, medium-sized and larger facilities, and OCS facilities 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 U.S.-flagged vessels, facilities, and OCS facilities might not have any cybersecurity measures in place. For the purpose of calculations in this analysis, we assume that all owners or operators of U.S.-flagged vessels, facilities, and OCS facilities will comply with the full extent of the requirements of this final rule, and we assume no waivers or exemptions outside of the population of U.S.-flagged barges with limited IT and OT systems. Cost estimates for requesting waivers or exemptions for U.S.-flagged barges are included in the Cybersecurity Plan development costs. For example, we assume that rather than taking the time to implement account security measures for nonexistent IT and OT systems, CySOs working for owners and operators of U.S.-flagged barges will use the time normally taken to document those measures to instead request a waiver and place the approval in their plan. As such, we include U.S.-flagged barges in our cost estimates for Cybersecurity Plan development and maintenance costs even though we do not include them in our estimates for the implementation of many of the cybersecurity measures analyzed later in the RA. Regarding waivers for implementing cybersecurity measures on other types of vessels or in facilities or OCS facilities, the Coast Guard is unable to estimate who in the affected population will request waivers and for which provisions. Instead, we discuss this as a source of uncertainty in table 42.

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.[96] We present this survey data in the applicable sections of the cost 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.

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 RA:

- Designation of a CySO in §§ 101.620(b)(3) and 101.630(c)(1);
- Device security measures in § 101.650(b)(1) through (4);
- Cybersecurity Assessment in § 101.650(e)(1);
- Letter certifying a completed penetration test and documentation of identified vulnerabilities in § 101.650(e)(2);
- Routine system maintenance measures in § 101.650(e)(3)(i) through (vi); and
- Supply chain management in § 101.650(f)(1) through (3);
- Development and maintenance of a Cyber Incident Response Plan in § 101.650(g)(2);
- Drafting of waiver or equivalence determination requests in § 101.665.

Developing a Cybersecurity Plan has five major 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 are required to submit their Cybersecurity Plan to the Coast Guard within 2 years following the effective date of this final rule; therefore, submitting a Cybersecurity Plan for approval will likely not occur until the second year of the 10-year period of analysis.

The CySO is responsible for all aspects of developing and maintaining the Cybersecurity Plan. While several public commenters indicated that they may need to hire a dedicated, salaried employee to serve as a CySO, the Coast Guard does not have specific data on what portion of owners and operators of vessels, facilities, and OCS facilities will need to do so. In this final rule, § 101.625 states that a CySO may serve in other roles and may perform other duties within an owner or operator's

[96] Readers can access the survey at *https://www.joneswalker.com/en/insights/2022-Jones-Walker-LLP-Ports-and-Terminals-Cybersecurity-Survey-Report.html,* accessed August 26, 2024.

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 FSO. For vessels, this person may be the VSO. 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 U.S.-flagged vessel, facility, or OCS facility company or organization will assume the duties and responsibilities of a CySO. This means that, while the Coast Guard is not requiring any security credentials for the CySO at this time, any costs associated with obtaining security credentials at the discretion of the owner or operator would already be incurred before the implementation of this final rule. Additionally, if the designated CySO has security responsibilities that overlap with an existing VSO, FSO, or CSO, we assume that those individuals will work together to handle those duties.

Despite our assumption that owners and operators will redesignate an existing employee, we acknowledge that some owners or operators may need to hire a CySO if no existing employees are able take on these duties. However, rather than estimating the hours associated with bringing on a full-time employee, the hour burdens associated with CySO duties have been quantified in various sections of the cost analysis. This can capture the costs associated with contracting for the individual CySO duties or assigning them to a new or existing employee.

We use the Bureau of Labor Statistics' (BLS) Occupational Employment and Wage Statistics (OEWS) for the United States for May 2022. A CySO is comparable to the occupational category of ''Information Security Analysts'' with an occupational code of 15–1212 and an unloaded mean hourly wage rate of $57.63.[97] In order to obtain a loaded mean hourly wage rate, we use BLS's ''Employer Costs for Employee Compensation'' database to calculate the load factor, which we applied to the unloaded mean hourly wage rate using fourth quarter data from 2022.[98] 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 final rule requires 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 MISLE database, we estimate this final rule will affect about 3,685 facilities and 33 OCS facilities (including MTSA-regulated facilities), and about 1,372 owners and operators of these facilities. MISLE data contains incomplete information on owners and operators for 951 of the 3,718 facilities and OCS facilities included in the affected population. Of the 2,767 facilities and OCS facilities with complete information for owners and operators, we found 1,055 unique owners. This means that, on average, each owner owns approximately 3 facilities (2,767 ÷ 1,055 = 2.62, or 3.0 rounded). We apply this rate of ownership to the remaining facilities and OCS facilities without complete ownership information to arrive at our total of 1,372 owners [1,055 + (951 ÷ 3)].

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 in ICR 1625–0077 include 100 hours for developing the Cybersecurity Plan (average hour burden), 10 hours for annual maintenance of the Cybersecurity Plan (which includes amendments), and 15 hours to resubmit Cybersecurity Plans every 5 years. In addition, SMEs estimate that it takes 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 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.

Based on estimates from the Coast Guard's FSP reviewers at local inspections offices, approximately 10 percent of Plans will 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 will 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 facilities and OCS facilities to be about $31,283,252 (3,718 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 $1,565,004 (372 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

[97] 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 August 22, 2024.

[98] 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 the ECEC Multi-Screen database tool at *https://data.bls.gov/multi-screen?survey=cm*. We then selected the category of ''2 Private industry workers'' at screen 1. At screen 2, we first selected the category ''01 Total compensation,'' then we continued to select ''530000 Transportation and materials moving occupations'' at screen 3, then ''All Workers'' at screens 4 and 5, and then for ''Area,'' we selected ''99999 United States (National)'' at screen 6. At screen 7, we selected the category ''D Cost of compensation (Cost per hour worked).'' 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 ''02 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 August 15, 2024.

develop, submit, and resubmit a Cybersecurity Plan to be approximately $32,848,256 ($31,283,252 + $1,565,004)).

In years 3 through 6 and years 8 through 10 of the analysis period, owners and operators of facilities and OCS facilities will 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 is 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 final rule also requires owners and operators of facilities and OCS facilities to conduct annual audits. The audits will be necessary for owners and operators of facilities and OCS facilities to identify vulnerabilities (via the Cybersecurity Assessment) and to mitigate them.[99] Audits will 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 is responsible for ensuring the audit of a Cybersecurity Plan, and we assume that an individual of similar experience and wage rate will conduct the annual audit. 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 owners and operators of facilities and OCS facilities to be approximately $3,128,325 (3,718 facility Plans × 10 hours × $84.14). We estimate the undiscounted cost for annual audits of Cybersecurity Plans to be approximately $12,513,301 (3,718 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 $15,641,626 ($3,128,325 + $12,513,301).

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 will be required to renew the approval of their Plans with the Coast Guard. We use the hour-burden estimate in ICR 1625–0077 for 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 is 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 $4,927,238 [(3,718 facility Plans × 15 hours × $84.14) + (372 resubmitted facility Plans × 7.5 hours × $84.14)].

We estimate the total discounted cost of this final rule for developing Cybersecurity Plans for owners and operators of facilities and OCS facilities to be approximately $132,678,949 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $14,770,687, using a 2-percent discount rate. See table 7. We estimate that the subset of 33 OCS facilities operated by 9 owners will incur costs of $1,176,239 over a 10-year period of analysis and $130,947 annualized, using a 2-percent discount rate.

BILLING CODE 9110–04–P

[99] The Jones Walker survey (see footnote 60) 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 August 26, 2024.

BILLING CODE 9110–04–C

Table 7: Estimated Cost of the Final Rule for Developing Cybersecurity Plans for Facilities and OCS Facilities (2022 Dollars, 10-year Period of Analysis, 2-percent Discount Rate)

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)]	2 Percent
1	1372	3718	0	$84.14	50	0	0	0	$15,641,626	$15,334,927
2	1372	3718	372	$84.14	50	0	50	0	$17,206,630	$16,538,476
3	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$14,739,454
4	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$14,450,445
5	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$14,167,103
6	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$13,889,316
7	1372	3718	372	$84.14	15	0	7.5	0	$4,927,238	$4,289,457
8	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$13,349,977
9	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$13,088,213
10	1372	3718	0	$84.14	0	10	0	40	$15,641,626	$12,831,581
Total									**$147,266,876**	**$132,678,949**
Annualized										**$14,770,687**

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 facilities and OCS facilities. We estimate the affected vessel population to be about 11,222. We estimate the number of owners and operators of these vessels to be about 2,075.

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 in ICR 1625–0077 include 80 hours for developing the Cybersecurity Plan, 8 hours for annual Plan maintenance, and 12 hours to renew the Plan every 5 years. In addition, Coast Guard SMEs estimate that it takes 40 hours to conduct annual audits of Plans for vessels. Similar to facilities, we estimate 10 percent of all Cybersecurity Plans for vessels will need to be resubmitted for corrections in the second year (initial year of Plan submission), and 10 percent of Cybersecurity Plans for vessels will 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 will 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 will 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 will 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 final rule will 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 will 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 will 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.

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 $13,967,240 (2,075 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 $700,045 (208 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 $14,667,285 ($13,967,240 + $700,045).

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, will 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 final rule also requires owners and operators of U.S.-flagged vessels to conduct annual audits. The audits will be necessary for owners and operators of U.S.-flagged vessels to identify vulnerabilities through the Cybersecurity Assessment and to mitigate them. Audits will 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 includes 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 $1,396,724 (2,075 Plans × 8 hours × $84.14). We estimate the undiscounted cost for annual audits of Cybersecurity Plans to be approximately $6,983,620 (2,075 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 $8,380,344 ($1,396,724 + $6,983,620).

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 will 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 is 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 $2,200,093 [(2,075 Plans × 12 hours × $84.14) + (208 resubmitted vessel Plans × 6 hours × $84.14)].

We estimate the total discounted cost of this final rule for owners and operators of U.S.-flagged vessels to develop Cybersecurity Plans to be approximately $67,857,908 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $7,554,385, using a 2-percent discount rate. See table 8.

BILLING CODE 9110–04–P

BILLING CODE 9110–04–C

Table 8: Estimated Cost of the Final Rule for Developing the Cybersecurity Plan for U.S.-flagged Vessels (2022 Dollars, 10-year Period of Analysis, 2-percent Discount Rate)

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)]	2 Percent
1	2075	2075	0	$84.14	40	0	0	0	$6,983,620	$6,846,686
2	2075	2075	208	$84.14	40	0	40	0	$7,683,665	$7,385,299
3	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$7,896,985
4	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$7,742,142
5	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$7,590,336
6	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$7,441,506
7	2075	2075	208	$84.14	12	0	6	0	$2,200,093	$1,915,313
8	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$7,152,543
9	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$7,012,297
10	2075	2075	0	$84.14	0	8	0	40	$8,380,344	$6,874,801
Total									**$75,529,786**	**$67,857,908**
Annualized										**$7,554,385**

Note: Totals may not sum due to independent rounding.

Drills

In § 101.635(b), this final rule requires drills that test the proficiency of U.S.-flagged vessel, facility, and OCS facility personnel who have assigned cybersecurity duties and individual elements of the Plan, including responses to cybersecurity threats and incidents. The drills enable the CySO to identify any cybersecurity deficiencies that need to be addressed. The CySO will need to conduct the drills at least twice annually, and they may be held in conjunction with other security or non-security-related drills, as appropriate. After considering public comments, in this final rule, we have adjusted the frequency of conducting drills from quarterly to twice each calendar year. We believe that two drills annually will ensure sufficient proficiency with the procedures, while allowing for a regulated entity to conduct additional drills if they choose to, and we understand how quarterly drills and exercises could be too frequent for some vessel operations, as noted by some commenters.

While there are benefits of a more robust drill schedule, we believe that this reduction in the number of drills lowers costs and increases marginal benefits by allowing affected owners and operators to use resources more efficiently. Further, by having fewer drills to develop and conduct, we believe the remaining drills will be the primary focus, addressing the commenter's concern about the previously proposed frequency and integration of cyber drills with other required drills. However, the Coast Guard believes that anything less frequent than two drills per year could lead to a decrease in benefits that drills provide. This is especially true with regard to cybersecurity, as risk and vulnerabilities can change rapidly over the course of a year.

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 will need to develop new cybersecurity related drills to comply with the requirements. While owners and operators in the affected population are allowed to combine these new cybersecurity drills with the drills required in accordance with 33 CFR parts 104, 105, and 106, several commenters suggested that combining these drills would be difficult or impossible. Accordingly, we have updated our cost estimates to reflect a longer time to develop and conduct drills and include employee participation in the new drills. Coast Guard SMEs who are familiar with MTSA's requirements and practices for drills and exercises, as well as Coast Guard SMEs at LANTAREA who have reviewed current drills in the affected population estimate that it will take a CySO 8 hours to develop each new cybersecurity drill.

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

In addition to the development costs, we also estimate the costs of employee participation in the cybersecurity drills. Coast Guard SMEs who are familiar with MTSA's requirements and practices for drills and exercises, as well as Coast Guard SMEs at LANTAREA who have reviewed current cybersecurity drills in the affected population estimate that each drill requires 4 hours of participation per employee. According to § 101.635(a)(1), drills and exercises must be used to test the proficiency of personnel in assigned cybersecurity duties. Because the Coast Guard is unable to determine which employees at a given facility or OCS facility will be in assigned cybersecurity duties and required to participate in the drills, we assume that 33 percent of employees will participate.[100] This share of employees is consistent with the estimated share of shoreside employees in the affected population of owners and operators of U.S.-flagged vessels. Coast Guard SMEs with knowledge of existing cybersecurity drill practices believe this is a more reasonable estimate than assuming the entire portion of employees will participate. We obtain the average number of facility employees from a Coast Guard contract that uses D&B Hoovers' database for company employee data (spreadsheet analysis available in the docket for this rulemaking, see file titled ''facilities_hoovers_employee_counts''). The average number of employees at a facility company is 74. We estimate that the average number of employees that will participate in cybersecurity drills is 24 (74 employees × 0.33 = 24.42).

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.[101] 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 ($41.33 × 1.46).

We estimate the cost for facilities to develop and conduct cybersecurity drills by using the number of owners and operators of facilities we presented earlier (1,372), the CySO's loaded mean hourly wage rate, the estimated time to develop the drill's components (8 hours), the estimated time to participate in the drills (4 hours), the average number of employees at a facility company (24 employees), the facility employee wage, and the frequency of the drill (twice annually).[102] We estimate the undiscounted annual cost for owners and operators of facilities and OCS facilities to develop, conduct, and participate in drills to be approximately $17,742,045 [1,372 facility companies × ((2 drills per year × 8 hours per drill development × $84.14 CySO wage) + (2 drills per year × 4 hours drill participation × 24 facility employees × $60.34 facility employee wage))]. We estimate the total discounted cost of drills for owners and operators of facilities and OCS facilities to be approximately $159,369,428 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the

[100] Under § 101.635(a)(1), cybersecurity drills and exercises are required to test the proficiency of U.S.-flagged vessel, facility, and OCS facility personnel in assigned cybersecurity duties. Full participation in drills and exercises from all personnel, including those without assigned cybersecurity duties, is not a requirement of this final rule.

[101] Readers can access this web page at *www.bls.gov/cew/*. Select the dropdown under ''QCEW data'' and click ''Databases.'' On this page, select the one-screen tool (*https://data.bls.gov/PDQWeb/en*). In fields 1 and 2, select ''U.S. TOTAL.'' In field 3, select ''NAICS 488310 Port and harbor operations.'' Select ''Private,'' ''All establishment sizes,'' and ''Average Weekly Wage'' in fields 4, 5, and 6, respectively. Click ''Add to selection'' and then ''Get Data.'' Relevant Series ID is ENUUS000405488310). For this RA, we used Q1 2022 QCEW data. We use the average weekly wage here because this QCEW database does not contain mean hourly wage data, accessed on August 15, 2024.

[102] For the purposes of capturing the cost of the CySO delivering the drill, we assume that the CySO is averaged into the number of employees participating in the drill. As such, we do not estimate a separate cost for CySO delivery of the drill.

annualized cost to be approximately $17,742,045, using a 2-percent discount rate. See table 9. We estimate that the subset of 33 OCS facilities operated by 9 owners will incur costs of $1,045,430 over a 10-year period of analysis and $116,384 annualized, using a 2-percent discount rate.

Table 9: Estimated Costs of the Final Rule for Drills for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Number of Facility Companies (a)	CySO Wage (b)	Drill Development Hours (c)	Hours to Conduct Drill (d)	Frequency of Drills (e)	Facility Employee Wage (f)	Number of Employees (g)	Total Cost = [a × ((b × c × e) + (d × e × f × g))]	2 Percent
1	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$17,394,162
2	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$17,053,100
3	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$16,718,725
4	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$16,390,907
5	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$16,069,517
6	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$15,754,428
7	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$15,445,518
8	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$15,142,665
9	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$14,845,750
10	1372	$84.14	8	4	2	$60.34	24	$17,742,045	$14,554,656
Total								$177,420,450	**$159,369,428**
Annualized									**$17,742,045**

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 2,075 CySOs, on behalf of owners and operators of U.S.-flagged vessels, who are required to develop drills with this final rule. As with facilities and OCS facilities, we have increased our development and hour-burden estimates, and now include cost estimates for a share of employees participating in cybersecurity drills. To determine the costs for employee participation, we use estimates for the number of employees per company and mean hourly wage estimates for employees based on vessel types.[103] We then subtract the total number of seafaring crew from the number of total company employees.[104] We use the estimated 33 percent ''shoreside'' share of employees for owners and operators of vessels because we do not have data on which portion of a given owner or operator's employees will have cybersecurity responsibilities. We feel this is more in line with the requirements of the regulatory text than assuming that all employees would participate. It also better aligns with suggestions from a public commenter who stated that ''onboard personnel have little to no involvement in cyber specific drills.''

For the vessel employee wage estimates, we chose several representative labor categories of vessel employees based on the manning requirements listed in the certificates of inspection for each vessel.[105] 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.[106] 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 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, in the docket of this rulemaking, for more details on how the industrial personnel and weighted mean hourly wages for

[103] 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 owners and operators of MTSA-regulated vessels who 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 owners and operators of MTS-regulated vessels. 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.

[104] For example, the average OSV in the affected population carries 12 seafaring crew per vessel according to certificate of inspection manning requirements. We multiply this by 1.33 to arrive at 16 total employees per OSV. We then subtract the 12 seafaring crew from the 16 total employees to isolate the 4 shoreside employees per vessel that would need to participate in the cybersecurity drills.

[105] Manning requirements for U.S.-flagged vessels were established by regulation in 46 CFR part 15.

[106] See *https://www.bls.gov/oes/2022/may/oes_nat.htm#00-0000* for 2022 wage rates associated with the listed occupations, accessed August 22, 2024.

each vessel type were calculated.[107] 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 10.

Table 10: Estimated Weighted Mean Hourly Wage Rates for Employees On board U.S.-flagged Vessels[108]

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

We estimate the undiscounted annual cost of cybersecurity drill participation for vessel employees to be approximately $12,644,432 (number of vessels for each affected vessel category × number of employees for each vessel type × representative mean hourly wage for vessel type × 4 hours for drill participation × 2 drills per year).[109] For example, using OSVs, there are about 430 OSVs, with 4 shoreside employees for each OSV. Therefore, we estimate the annual drill participation cost for OSVs to be about $755,699 (430 OSVs × 4 shoreside employees × $54.92 × 4 hours × 2 drills), rounded. We perform this calculation for all for the affected vessel types in this final rule and add it to the estimated costs for drill development. We estimate the undiscounted annual cost to develop cybersecurity drills to be approximately $2,793,448 (2,075 vessel companies × 1 CySO per vessel company × $84.14 × 8 hours to develop drills × 2 drills per year)]. This means the total undiscounted annual drill cost for the affected population of U.S.-flagged vessels is $15,437,880 ($12,644,432 drill participation costs + $2,793,448 drill development costs). Table 11 displays the total employee drill participation costs for each vessel type impacted by the drill requirement.

[107] 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 given population of vessels.

[108] See Appendix A: Wages Across Vessel Types for more information on how these wages rates were calculated.

[109] To capture the cost of the CySO delivering the drill, we assume that the CySO is averaged into the number of employees participating in the drill. As such, we do not estimate a separate cost for CySO delivery of the drill.

Table 11: Estimated Costs of the Final Rule for Drill Participation by Vessel Type for U.S.-flagged Vessels (2022 Dollars, Undiscounted Costs)

Vessel Type	Number of Vessels	Number of Shoreside Employees per Vessel	Drill Wage	Number of Drills per year	Hours to Complete Drills per Year	Total
MODU	1	92	$39.60	2	4	$29,146
Subchapter I Vessels	398	20	$46.36	2	4	$2,952,205
OSVs	430	4	$54.92	2	4	$755,699
Subchapter H Passenger Vessels	131	21	$41.85	2	4	$921,035
Subchapter K Passenger Vessels	430	9	$45.52	2	4	$1,409,299
Subchapter M Towing Vessels	4822	3	$51.28	2	4	$5,934,532
Subchapter D and Combination O&D Tank Vessels	114	10	$55.94	2	4	$510,173
Subchapters K and T International Passenger Vessels	53	7	$44.59	2	4	$132,343
Total						**$12,644,432**

We estimate the total discounted cost of drills for U.S.-flagged vessels to be approximately $138,672,070 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $15,437,880, using a 2-percent discount rate. See table 12.

Table 12: Estimated Costs of the Final Rule for Drills for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Total Cost	2 Percent
1	$15,437,880	$15,135,176
2	$15,437,880	$14,838,408
3	$15,437,880	$14,547,459
4	$15,437,880	$14,262,215
5	$15,437,880	$13,982,564
6	$15,437,880	$13,708,396
7	$15,437,880	$13,439,604
8	$15,437,880	$13,176,082
9	$15,437,880	$12,917,727
10	$15,437,880	$12,664,439
Total	$154,378,800	**$138,672,070**
Annualized		**$15,437,880**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of this final rule for drills for the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to be approximately $298,041,496 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $33,179,925, using a 2-percent discount rate. See table 13.

Table 13: Estimated Costs of the Final Rule for Drills for U.S.-flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year period of Analysis, 2-percent Discount Rate)

Year	Facilities Drill Cost	Vessel Drill Cost	Total Cost	2 Percent
1	$17,742,045	$15,437,880	$33,179,925	$32,529,338
2	$17,742,045	$15,437,880	$33,179,925	$31,891,508
3	$17,742,045	$15,437,880	$33,179,925	$31,266,184
4	$17,742,045	$15,437,880	$33,179,925	$30,653,122
5	$17,742,045	$15,437,880	$33,179,925	$30,052,080
6	$17,742,045	$15,437,880	$33,179,925	$29,462,824
7	$17,742,045	$15,437,880	$33,179,925	$28,885,121
8	$17,742,045	$15,437,880	$33,179,925	$28,318,747
9	$17,742,045	$15,437,880	$33,179,925	$27,763,477
10	$17,742,045	$15,437,880	$33,179,925	$27,219,095
Total	$177,420,450	$154,378,800	$331,799,250	**$298,041,496**
Annualized				**$33,179,925**

Note: Totals may not sum due to independent rounding.

Exercises

In § 101.635(c), this final rule requires 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 are 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 must 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) will 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. In addition, because the affected populations are already required to conduct exercises per §§ 104.230, 105.220, and 106.225, this final rule allows for owners and operators to hold cybersecurity exercises in conjunction with other exercises. However, based on suggestions from public commenters, the size and scope of these exercises may make them difficult to combine in all cases. Due to a lack of data on who will be able to combine exercises, we assume that the entire populations will need to develop new cybersecurity-related exercises to comply with the requirements. In either case, these development and participation hour-burden estimates could cover the development of new internal exercises, or preparation and participation in local area exercises.

Coast Guard SMEs who are familiar with MTSA's requirements and practices for drills and exercises, Coast Guard SMEs at LANTAREA who have reviewed current exercises in the affected population, and Coast Guard SMEs at Sector San Juan who worked to develop cybersecurity exercises with the local AMSC estimate that it takes a CySO 20 hours on average to develop new functional, full scale cybersecurity exercises. We have increased our hour-burden estimate for developing exercise components from 8 hours in the NPRM to 20 hours in the final rule to reflect the development of full-scale exercises since we no longer assume that they will be combined with existing exercises. It should be noted that CySOs can access widely available resources and planning materials for developing cybersecurity exercises online.[110] In addition, the proliferation of cybersecurity components already being added to AMSC exercises around the United States provide examples for CySOs working to develop their own exercises.[111]

We assume each CySO, on behalf of the owner and operator of a facility or OCS facility, will develop the exercises specified in this final rule. Using the 1,372 facility owners and operators we presented earlier, the CySO's loaded mean hourly wage rate, the 20-hour estimate for developing the exercise, and one annual exercise, we estimate the cost for facilities to develop cybersecurity exercise components. We estimate the undiscounted annual cost of exercises for owners and operators of facilities and OCS facilities to be approximately $2,308,802 (1,372 facility CySOs × 20 hours per exercise × $84.14 CySO wage).

In addition to the development costs, we also estimate the costs of employee participation in the cybersecurity exercises. Coast Guard SMEs who are

[110] For example, CISA offers free resources on cybersecurity scenarios and cybersecurity exercises on their website. See *https://www.cisa.gov/cybersecurity-training-exercises,* accessed August 22, 2024.

[111] See *https://digitaleditions.walsworthprintgroup.com/publication/?i=459304&article_id=2956672&view=articleBrowser* and *https://www.news.uscg.mil/Press-Releases/Article/3920011/coast-guard-area-maritime-security-partners-conduct-2-cyber-security-exercises/* for just two examples of AMSC cyber exercises in recent years, accessed August 22, 2024.

familiar with MTSA's requirements and practices for drills and exercises, Coast Guard SMEs at LANTAREA who have reviewed current cybersecurity drills in the affected population, and Coast Guard SMEs at Sector San Juan who worked to develop cybersecurity exercises with the local AMSC estimate that each exercise requires 4 hours of participation per employee. This is based on the average length of time it took to lead and administer local AMSC cybersecurity exercises.[112]

According to § 101.635(a)(1), drills and exercises must be used to test the proficiency of personnel in assigned cybersecurity duties. Because the Coast Guard is unable to determine which employees at a given facility or OCS facility will be in assigned cybersecurity duties and required to participate in the exercises, we assume that 33 percent of employees will participate.[113] This share of employees is consistent with the estimated share of shoreside employees in the affected population of owners and operators of U.S.-flagged vessels. Coast Guard SMEs with knowledge of existing cybersecurity exercise practices believe this is a more reasonable estimate than assuming the entire portion of employees will participate. We estimate that the average number of employees that will participate in cybersecurity exercises is 24 (74 total employees × 0.33 = 24.42) with a loaded mean hourly wage of $60.34.

We estimate the cost for facilities to develop and conduct cybersecurity exercises by using the number of facilities owners and operators we presented earlier (1,372), the CySO's loaded mean hourly wage rate, the estimated time to develop the exercise components (20 hours), the estimated time to participate in the exercises (4 hours), the average number of participating employees at a facility company (24 employees), and the facility employee wage.[114]

We estimate the undiscounted annual cost for owners and operators of facilities and OCS facilities to develop and conduct exercises to be approximately $10,256,304 [1,372 facility companies × ((20 hours exercise development × $84.14 CySO wage) + (4 hours exercise participation × 24 facility employees × $60.34 facility employee wage))].[115] We estimate the total discounted cost of exercises for owners and operators of facilities and OCS facilities to be approximately $92,128,123 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $10,256,304, using a 2-percent discount rate.

We estimate that the subset of 33 OCS facilities operated by 9 owners will incur costs of $604,339 over a 10-year period of analysis and $67,279 annualized, using a 2-percent discount rate. See table 14.

[112] We estimate similar lengths of participation time for both exercises and drills because, while drills are meant to test individual elements of the Cybersecurity Plan and exercises are required to be a full test of the cybersecurity program, depending on what is being drilled, drills can be more open-ended or involve lengthy and in-depth practice of incident response and recovery procedures. Consider a suite of cybersecurity drills that includes phishing attack simulations, which would involve the CySO sending false emails from a seemingly trusted source in order to extract personal identifying information from recipients. For example, a mock phishing email can have an attachment or link that alerts the testing team when it's opened, or can include a link that goes to a mock login page. This will allow the CySO to see how many people not only click the link but also insert their credentials. Drilling through this scenario could take hours to wait and see who interacts with the email, record results, and assemble their team to discuss lessons learned and response procedures if the phishing attempt is successful. While only an example, drilling one of these scenarios (or another like it) in-depth can require a similar length of time as a full exercise when considering time to conduct the drill, record results, practice response procedures, and discuss lessons learned as a team.

[113] Under § 101.635(a)(1), cybersecurity drills and exercises are required to test the proficiency of U.S.-flagged vessel, facility, and OCS facility personnel in assigned cybersecurity duties. Full participation in drills and exercises from all personnel, including those without assigned cybersecurity duties, is not a requirement of this final rule.

[114] To capture the cost of the CySO delivering the exercise, we assume that the CySO is averaged into the number of employees participating in the exercise. As such, we do not estimate a separate cost for CySO delivery of the exercise.

[115] To capture the cost of the CySO administering the exercise, we assume that the CySO is averaged into the number of employees participating in the exercise. As such, we do not estimate a separate cost for CySO delivery of the exercise.

Table 14: Estimated Costs of the Final Rule for Exercises for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Number of Facility Companies (a)	CySO Wage (b)	Exercise Development Hours (c)	Exercise Participation Hours (d)	Facility Employee Wage (e)	Number of Employees (f)	Total Cost = [a × ((b × c) + (d × e × f))]	2 Percent
1	1372	$84.14	20	4	$60.34	24	$10,256,304	$10,055,200
2	1372	$84.14	20	4	$60.34	24	$10,256,304	$9,858,039
3	1372	$84.14	20	4	$60.34	24	$10,256,304	$9,664,744
4	1372	$84.14	20	4	$60.34	24	$10,256,304	$9,475,240
5	1372	$84.14	20	4	$60.34	24	$10,256,304	$9,289,451
6	1372	$84.14	20	4	$60.34	24	$10,256,304	$9,107,304
7	1372	$84.14	20	4	$60.34	24	$10,256,304	$8,928,730
8	1372	$84.14	20	4	$60.34	24	$10,256,304	$8,753,657
9	1372	$84.14	20	4	$60.34	24	$10,256,304	$8,582,016
10	1372	$84.14	20	4	$60.34	24	$10,256,304	$8,413,742
Total							$102,563,040	**$92,128,123**
Annualized								**$10,256,304**

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 2,075 CySOs, on behalf of vessel owners and operators, will be required to conduct exercises with this final rule. As with facilities and OCS facilities, we have increased our development hour-burden estimates, and now include cost estimates for shoreside employees participating in cybersecurity exercises. To determine the costs for employee participation, we use estimates for the number of employees per company and mean hourly wage estimates for employees based on vessel types previously calculated in our analysis of cybersecurity drill costs. See table 10 for a breakdown of the mean hourly wage estimates used for employees in the U.S.-flagged vessel population.

We estimate the undiscounted annual cost of cybersecurity exercise participation for vessel employees to be approximately $6,322,216 (number of vessels for each affected vessel category × number of employees for each vessel type × representative mean hourly wage for vessel type × 4 hours for exercise participation).[116] For example, using OSVs, there are about 430 OSVs, with 4 shoreside employees for each OSV. Therefore, we estimate the annual exercise participation cost for OSVs to be about $377,850 (430 OSVs × 4 shoreside employees × $54.92 employee wage × 4 hours), rounded. We perform this calculation for all for the affected vessel types in this final rule and add it to the estimated costs for exercise development. We estimate the undiscounted annual cost to develop cybersecurity exercises to be approximately $3,491,810 (2,075 vessel companies × 1 CySO per vessel company × $84.14 CySO wage × 20 hours to develop exercises)]. This means the total undiscounted annual exercise cost for the affected population of U.S.-flagged vessels is $9,814,026 ($6,322,216 exercise participation costs + $3,491,810 exercise development costs). Table 15 displays the total employee exercise participation costs for each vessel type impacted by the exercise requirement.

[116] To capture the cost of the CySO administering the exercise, we assume that the CySO is averaged into the number of employees participating in the exercise. As such, we do not estimate a separate cost for CySO delivery of the exercise.

Table 15: Estimated Costs of the Final Rule for Exercise Participation by Vessel Type for U.S.-flagged Vessels (2022 Dollars, Undiscounted Costs)

Vessel Type	Number of Vessels	Number of Shoreside Employees	Employee Wage	Number of Exercises	Hours to Complete Exercises per Year	Total
MODU	1	92	$39.60	1	4	$14,573
Subchapter I Vessels	398	20	$46.36	1	4	$1,476,102
OSVs	430	4	$54.92	1	4	$377,850
Subchapter H Passenger Vessels	131	21	$41.85	1	4	$460,517
Subchapter K Passenger Vessels	430	9	$45.52	1	4	$704,650
Subchapter M Towing Vessels	4822	3	$51.28	1	4	$2,967,266
Subchapter D and Combination O&D Tank Vessels	114	10	$55.94	1	4	$255,086
Subchapters K and T International Passenger Vessels	53	7	$44.59	1	4	$66,172
Total						**$6,322,216**

We estimate the total discounted cost of exercises for U.S.-flagged vessels to be approximately $88,155,323 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $9,814,026, using a 2-percent discount rate. See table 16.

Table 16: Estimated Costs of the Final Rule for Exercises for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Total Cost	2 Percent
1	$9,814,026	$9,621,594
2	$9,814,026	$9,432,935
3	$9,814,026	$9,247,976
4	$9,814,026	$9,066,643
5	$9,814,026	$8,888,866
6	$9,814,026	$8,714,574
7	$9,814,026	$8,543,700
8	$9,814,026	$8,376,177
9	$9,814,026	$8,211,938
10	$9,814,026	$8,050,920
Total	$98,140,260	**$88,155,323**
Annualized		**$9,814,026**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of this final rule for the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities for exercises to be approximately $180,283,445 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $20,070,330, using a 2-percent discount rate. See table 17.

Table 17: Estimated Cost of the Final Rule for Exercises for U.S.-flagged Vessels Facilities, and OCS Facilities (2022 Dollars, 10-year Period of Analysis, 2-percent Discount Rate)

Year	Facilities Exercise Cost	Vessel Exercise Cost	Total Cost	2 Percent
1	$10,256,304	$9,814,026	$20,070,330	$19,676,794
2	$10,256,304	$9,814,026	$20,070,330	$19,290,975
3	$10,256,304	$9,814,026	$20,070,330	$18,912,720
4	$10,256,304	$9,814,026	$20,070,330	$18,541,883
5	$10,256,304	$9,814,026	$20,070,330	$18,178,316
6	$10,256,304	$9,814,026	$20,070,330	$17,821,879
7	$10,256,304	$9,814,026	$20,070,330	$17,472,430
8	$10,256,304	$9,814,026	$20,070,330	$17,129,833
9	$10,256,304	$9,814,026	$20,070,330	$16,793,954
10	$10,256,304	$9,814,026	$20,070,330	$16,464,661
Total	$102,563,040	$98,140,260	$200,703,300	**$180,283,445**
Annualized				**$20,070,330**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost of this final rule for the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to conduct annual drills and exercises to be approximately $478,324,941 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $53,250,255, using a 2-percent discount rate. See table 18.

Table 18: Summary of Discounted Costs of the Final Rule for Drills and Exercises (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

	Facilities and OCS Facilities	U.S.-flagged Vessels	Total Cost	2 Percent
Drills	$177,420,450	$154,378,800	**$331,799,250**	**$298,041,496**
Exercises	$102,563,040	$98,140,260	**$200,703,300**	**$180,283,445**
Total	$279,983,490	$252,519,060	**$532,502,550**	**$478,324,941**
Annualized				**$53,250,255**

Note: Totals may not sum due to independent rounding.

Cybersecurity Measure Costs

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

The first provision is account security measures in § 101.650(a). The owners and operators of each U.S.-flagged vessel, facility, and OCS facility will ensure that account security measures are implemented and documented. This includes general account security measures in § 101.650(a)(1) through (3) and (5) through (7) and multifactor authentication for end users in § 101.650(a)(4). Based on the Jones Walker ''Ports and Terminals Cybersecurity Survey,'' (see footnote 60), 87 percent of facilities currently have account security measures, and 83 percent of facilities currently use multifactor authentication software. Using the total number of 1,372 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 need to implement security measures and have multifactor authentication software under this final rule, or about 178 and 233, respectively.

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 ensures that account security measures are implemented. Using wage data from the BLS OEWS program as previously referenced, the unloaded mean hourly wage rate for this labor category, occupational code of 15–1242, is $49.29.[117] 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 takes a database administrator about 8 hours to implement the account security measures and 8 hours for account security management annually thereafter for 178 facility and OCS facility companies. We estimate the undiscounted initial-year cost to implement account security for 178 facilities and OCS facilities and the annually recurring cost of account security management to be approximately $102,471, rounded [(178 facility companies × ($71.96 × 8 hours)].

The number of facility and OCS facility companies that will need multifactor authentication security is about 233. Based on estimates from CG–FAC SMEs with experience implementing multifactor authentication at other Government agencies, implementation of multifactor authentication will cost each facility anywhere from $3,000 to $15,000 in the initial year for setup and configuration. For this RA, we use the average of approximately $9,000 for the costs of initial setup and configuration. It will 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 will need multifactor authentication, and (2) whether only a subset of the total employees will 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 RA, we assume all employees will need multifactor authentication access.

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). The average number of employees at a facility company is 74. We estimate the undiscounted initial-year cost to implement multifactor authentication for 233 facility and OCS facility companies to be approximately $2,097,000 (233 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 $2,586,300 (233 facility companies × 74 employees × $150).

We estimate the total undiscounted initial-year cost to implement account security measures and multifactor authentication for facilities and OCS facilities to be approximately $4,785,771 ($102,471 cost to implement account security measures + $2,097,000 cost to set up and configure multifactor authentication + $2,586,300 cost for multifactor authentication support). We estimate the undiscounted annual cost in Years 2 through 10 to be approximately $2,688,771 ($102,471 cost to manage account security + $2,586,300 cost to maintain and provide multifactor authentication support).

We estimate the total discounted cost to implement account security measures for (1) 178 facilities and OCS facilities that will need to implement general account security measures and (2) 233 facilities and OCS facilities that will need to implement multifactor authentication to be approximately

[117] See *https://www.bls.gov/oes/2022/may/oes151242.htm,* accessed August 22, 2024.

$26,207,997 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $2,917,645, using a 2-percent discount rate.

Using the same rates of baseline activity for the total population of facilities, we estimate that a subset of (1) 1 OCS facility owner or operator that will need to implement general account security measures and (2) 2 OCS facility owners or operators that will need to implement multifactor authentication to be approximately $222,234 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $24,741, using a 2-percent discount rate. See table 19.

Table 19: Estimated Costs of the Final Rule for Account Security Measures and Multifactor Authentication for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Account Security Measure Costs	Multifactor Authentication Costs	Total Cost	2 Percent
1	$102,471	$4,683,300	$4,785,771	$4,691,932
2	$102,471	$2,586,300	$2,688,771	$2,584,363
3	$102,471	$2,586,300	$2,688,771	$2,533,689
4	$102,471	$2,586,300	$2,688,771	$2,484,009
5	$102,471	$2,586,300	$2,688,771	$2,435,303
6	$102,471	$2,586,300	$2,688,771	$2,387,552
7	$102,471	$2,586,300	$2,688,771	$2,340,737
8	$102,471	$2,586,300	$2,688,771	$2,294,840
9	$102,471	$2,586,300	$2,688,771	$2,249,843
10	$102,471	$2,586,300	$2,688,771	$2,205,729
Total			$28,984,710	**$26,207,997**
Annualized				**$2,917,645**

Note: Totals may not sum due to independent rounding.

Owners and operators of U.S.-flagged vessels will need to implement the same account security measures as facilities and OCS facilities. The population of vessels affected, where applicable, will be about 6,379, rather than 11,222, because we subtract the barge population of 4,843 from 11,222, the total number of affected vessels. Because barges are unmanned, we assume they do not have computer systems on board and, therefore, may not require account security measure implementation. Instead, we assume they will request waivers for these provisions, a cost included in Cybersecurity Plan development costs estimated earlier in the analysis.

The number of affected vessel owners and operators will be about 1,686, excluding 389 barge owners and operators that do not own or operate other affected vessels. Based on the NMSAC estimates detailed above, it will 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 $970,596 [(1,686 vessel owners and operators × (8 hours × $71.96)].

The number of owners and operators who will require multifactor authentication security is about 1,686, for approximately 6,379 vessels. Based on Coast Guard information, multifactor authentication systems will be implemented at the company level because networks and account security policies will be managed at the company level, and not for each individual vessel. Any security updates or multifactor authentication programs implemented at the company level can 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 will 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 as described in the cost analysis for cybersecurity drills. Similarly, we assume 2 crews and multiply the total number of seafaring crew by 1.33 to account for shoreside staff to obtain an estimate of total company employees per vessel. We estimate the total undiscounted initial-year cost to implement multifactor authentication for 1,686 vessel owners and operators to be approximately $15,174,000 (1,686 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 430 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 will be approximately $1,032,000 (16 employees per each OSV (including shoreside) × $150 × 430 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 $20,212,500 (number of employees for each vessel type × $150 × number of vessels for each vessel type). See table 20. We add these costs to the previously calculated implementation costs to obtain the initial-year costs associated with multifactor authentication of $35,386,500 ($15,174,000 implementation costs + $20,212,500 annual support and maintenance costs) as seen in column 3 of table 21.

Table 20: Estimated Annual Costs of the Final Rule for Multifactor Authentication Support and Maintenance for U.S.-flagged Vessel Companies by Vessel Type (2022 Dollars)

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	398	82	$150	$4,895,400
OSVs	430	16	$150	$1,032,000
Subchapter H Passenger Vessels	131	85	$150	$1,670,250
Subchapter K Passenger Vessels	430	35	$150	$2,257,500
Subchapter M Towing Vessels	4822	13	$150	$9,402,900
Subchapter D and Combination O&D Tank Vessels	114	40	$150	$684,000
Subchapters K and T International Passenger Vessels	53	27	$150	$214,650
Total				**$20,212,500**

Note: Totals may not sum due to independent rounding.

We estimate the total undiscounted initial-year cost to implement account security measures in § 101.650(a)(1) through (3), and (5) through (7) and multifactor authentication for end users in § 101.650(a)(4) for 1,686 owners and operators of U.S.-flagged vessels to be approximately $36,357,096 ($970,596 cost to implement account security + $35,386,500 cost to implement and provide multifactor support). We estimate the total undiscounted annual cost in Years 2 through 10 to be approximately $21,183,096 ($970,596 cost to manage account security + $20,212,500 cost to maintain and provide multifactor authentication).

We estimate the total discounted cost to implement all the account security measures in § 101.650(a)(1) through (3), and (5) through (7) and multifactor authentication for end users in § 101.650(a)(4) for 1,686 owners and operators of U.S.-flagged vessels to be approximately $205,155,431 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $22,839,242 using a 2-percent discount rate. See table 21.

Table 21: Estimated Costs of the Final Rule for Account Security Measures and Multifactor Authentication for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Account Security Measure Costs	Multifactor Authentication Costs	Total Cost	2 Percent
1	$970,596	$35,386,500	$36,357,096	$35,644,212
2	$970,596	$20,212,500	$21,183,096	$20,360,531
3	$970,596	$20,212,500	$21,183,096	$19,961,304
4	$970,596	$20,212,500	$21,183,096	$19,569,906
5	$970,596	$20,212,500	$21,183,096	$19,186,183
6	$970,596	$20,212,500	$21,183,096	$18,809,983
7	$970,596	$20,212,500	$21,183,096	$18,441,160
8	$970,596	$20,212,500	$21,183,096	$18,079,568
9	$970,596	$20,212,500	$21,183,096	$17,725,067
10	$970,596	$20,212,500	$21,183,096	$17,377,517
Total			$227,004,960	**$205,155,431**
Annualized				**$22,839,242**

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 $231,363,427 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $25,756,887, using a 2-percent discount rate. See table 22.

Table 22: Summary of Costs of the Final Rule for Account Security Measures and Multifactor Authentication for U.S.-flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Facilities and OCS Facilities Cost	U.S.-flagged Vessels Cost	Total Cost	2 Percent
1	$4,785,771	$36,357,096	$41,142,867	$40,336,144
2	$2,688,771	$21,183,096	$23,871,867	$22,944,893
3	$2,688,771	$21,183,096	$23,871,867	$22,494,993
4	$2,688,771	$21,183,096	$23,871,867	$22,053,915
5	$2,688,771	$21,183,096	$23,871,867	$21,621,485
6	$2,688,771	$21,183,096	$23,871,867	$21,197,535
7	$2,688,771	$21,183,096	$23,871,867	$20,781,897
8	$2,688,771	$21,183,096	$23,871,867	$20,374,409
9	$2,688,771	$21,183,096	$23,871,867	$19,974,910
10	$2,688,771	$21,183,096	$23,871,867	$19,583,246
Total			**$255,989,670**	**$231,363,427**
Annualized				**$25,756,887**

Note: Totals may not sum due to independent rounding.

Cybersecurity Training Cost

The second cost provision under cybersecurity measures, in § 101.650(d), will be training. All persons with access to IT and OT will 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 will be verified during annual inspections following the implementation of this final rule. This means we assume there will be costs related to training in the first year of analysis.

Based on information from the Jones Walker ''Ports and Terminals Cybersecurity Survey,'' (see footnote 60), about 25 percent of facilities are currently conducting cybersecurity training on an annual basis.[118] Therefore, we estimate the number of owners and operators of facilities and OCS facilities who need to implement training to be about 1,029 (1,372 owners and operators × 0.75).

Based on information from Coast Guard SMEs, we assume that the CySO at a facility or OCS facility will spend 2 hours per year to develop, update, and provide cybersecurity training. This is an average estimate based on the time it would take to either develop unique training or identify existing training resources to use within their organizations. This length of time will vary widely based on the complexity of the material and general familiarity with the subject matter but is aided by publicly available training resources online.[119] Subject matter experts with Coast Guard also estimate that it will take 1 hour per facility employee to complete the training annually, based on existing industry-leading cyber awareness training programs.[120]

This final rule will also require part-time employees and contractors to complete the training but allow for personnel unable to receive cybersecurity training to be accompanied or monitored by a person who has completed the required training when accessing IT or OT systems. However, the Coast Guard has data only on the number of full-time employees at facilities and OCS facilities, so we use this estimate. We acknowledge that costs may be higher for facilities than we estimate in this analysis if we take other employees into account. Missing from this estimate are part-time employees and contractors, and if pertinent, estimated costs for the unknown number of employees who will need to be accompanied when accessing IT or OT systems. If included, the training costs would be higher than currently estimated. However, it is possible that some of these individuals would already require an escort under 33 CFR part 105 for access to designated secure areas, and that this would not lead to any change in operations. As before, we use the estimate of the average number of employees at facilities and OCS facilities, or 74. We also use the previously calculated loaded mean hourly wage rate of approximately $60.34 for the facility employees.

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 $4,767,810, rounded [1,029 facility owners and operators × ((74 employees at each facility company × $60.34 facility employee wage × 1 hour) + (1 CySO developing training × $84.14 CySO wage × 2 hours))].

We estimate the discounted cost for facility and OCS facility owners and operators to complete annual training to be approximately $42,827,259 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $4,767,810, using a 2-percent discount rate. See table 23. Using the same rate of baseline activity estimated for the overall population of facilities, we estimate that the subset of 7 owners or operators of OCS facilities will incur costs of $291,340 over a 10-year period of analysis and $32,434 annualized, using a 2-percent discount rate.

[118] See footnote 60 and page 48 of the survey in the docket.

[119] For example, see CISA's compilation of Cybersecurity Education and Training Resources: *https://www.cisa.gov/sites/default/files/2024-02/Resources%20Collection_02062024_508c.pdf,* accessed October 11, 2024.

[120] In addition, CG–FAC recently worked with ABS to deliver Cybersecurity Awareness Training for AMSC members. This training took approximately 1 hour to deliver and is available here: *https://ww2.eagle.org/en/news/abs-news/abs-leads-cyber-trainings-for-us-coast-guard-maritime-security-committee-members.html,* accessed October 11, 2024.

Table 23: Estimated Training Costs of the Final Rule for Owners and Operators of Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rates)

Year	Total Cost	2 Percent
1	$4,767,810	$4,674,324
2	$4,767,810	$4,582,670
3	$4,767,810	$4,492,814
4	$4,767,810	$4,404,719
5	$4,767,810	$4,318,352
6	$4,767,810	$4,233,679
7	$4,767,810	$4,150,666
8	$4,767,810	$4,069,280
9	$4,767,810	$3,989,490
10	$4,767,810	$3,911,265
Total	$47,678,100	**$42,827,259**
Annualized		**$4,767,810**

Note: Totals may not sum due to independent rounding.

Employees on board U.S.-flagged vessels will 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 (excluding barges), similar to the cost analysis for drills and account security measures. Similarly, we use the loaded mean hourly wage rates shown in table 10 in our cost analysis for cybersecurity drills.

We estimate the undiscounted initial-year and annual cost of cybersecurity training for vessel employees to be approximately $6,590,094 (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 430 OSVs, with 16 employees for each OSV (including shoreside). Therefore, we estimate the annual training cost for OSVs to be about $377,850 (430 OSVs × 16 employees × $54.92 OSV employee wage × 1 hour), rounded. We perform this calculation for all for the affected vessel types in this final rule and add it to the estimated costs for training development. We estimate the undiscounted annual cost to develop cybersecurity training to be approximately $283,720 (1,686 vessel companies (excluding barge companies) × 1 CySO per vessel company × $84.14 CySO wage × 2 hours to develop training)]. This means the total undiscounted annual training cost for the affected population of U.S.-flagged vessels is $6,873,814 ($6,590,094 employee training costs + $283,720 training development costs). Table 24 displays the total employee training costs for each vessel type impacted by the training requirement.

Table 24: Estimated Training Costs of the Final Rule for U.S.-flagged Vessels by Vessel 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	398	82	$46.36	$1,513,005
OSVs	430	16	$54.92	$377,850
Subchapter H Passenger Vessels	131	85	$41.85	$466,000
Subchapter K Passenger Vessels	430	35	$45.52	$685,076
Subchapter M Towing Vessels	4822	13	$51.28	$3,214,538
Subchapter D and Combination O&D Tank Vessels	114	40	$55.94	$255,086
Subchapters K and T International Passenger Vessels	53	27	$44.59	$63,808
Total				**$6,590,094**

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 $61,744,618 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $6,873,814, using a 2-percent discount rate. See table 25.

Table 25: Estimated Training Costs of the Final Rule for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Total Cost	2 Percent
1	$6,873,814	$6,739,033
2	$6,873,814	$6,606,895
3	$6,873,814	$6,477,348
4	$6,873,814	$6,350,342
5	$6,873,814	$6,225,825
6	$6,873,814	$6,103,750
7	$6,873,814	$5,984,069
8	$6,873,814	$5,866,734
9	$6,873,814	$5,751,700
10	$6,873,814	$5,638,922
Total	$68,738,140	**$61,744,618**
Annualized		**$6,873,814**

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 $104,571,877 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $11,641,624, using a 2-percent discount rate. See table 26.

Table 26: Summary of Training Costs of the Final Rule for U.S.-flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Facilities and OCS Facilities	U.S.-flagged Vessels	Total Cost	2 Percent
1	$4,767,810	$6,873,814	$11,641,624	$11,413,357
2	$4,767,810	$6,873,814	$11,641,624	$11,189,566
3	$4,767,810	$6,873,814	$11,641,624	$10,970,162
4	$4,767,810	$6,873,814	$11,641,624	$10,755,061
5	$4,767,810	$6,873,814	$11,641,624	$10,544,178
6	$4,767,810	$6,873,814	$11,641,624	$10,337,429
7	$4,767,810	$6,873,814	$11,641,624	$10,134,734
8	$4,767,810	$6,873,814	$11,641,624	$9,936,014
9	$4,767,810	$6,873,814	$11,641,624	$9,741,190
10	$4,767,810	$6,873,814	$11,641,624	$9,550,186
Total	**$47,678,100**	**$68,738,140**	**$116,416,240**	**$104,571,877**
Annualized				**$11,641,624**

Note: Totals may not sum due to independent rounding.

Penetration Testing

The third provision under cybersecurity measures that will impose costs on industry is penetration testing, in § 101.650(e)(2). The CySO for each U.S.-flagged vessel, facility, and OCS facility will ensure that a penetration test is completed in conjunction with renewing the Cybersecurity Plan. We assume facility and vessel owners and operators in the affected population will 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 will also need to include a letter certifying the test was conducted and document all identified vulnerabilities in the FSA, OCS FSA, or VSA—a cost that is included in our analysis of annual Cybersecurity Plan maintenance. Further, it is expected that the CySO will 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 60), 68 percent of facilities and OCS facilities are currently conducting penetration testing. Using 1,372 affected owners and operators of facilities and OCS facilities, the number of owners and operators of facilities and OCS facilities who need to conduct penetration testing is about 439 (1,372 × 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, as well as Coast Guard SMEs with similar experience, we estimate it will cost each owner or operator of a facility or OCS facility $10,000 for the initial penetration test and an additional $100 for each IP address on the network to capture the additional costs of network complexity.

In the NPRM, we estimated initial costs of $5,000 for the penetration test, an additional $50 per IP address, and used the number of employees as a rough estimate for the number of IP addresses on a given network. We received several public comments on these estimates that suggested that we were underestimating the costs of penetration testing and the number of IP addresses by not including estimates for additional industrial personnel and OT systems. While none of the commenters provided specific cost estimates beyond stating that our estimates were underestimates, one comment from Offshore Marine Service Association stated that we did not include all relevant costs by assuming that there would be IP addresses equal to the number of employees at a company. In addition to crewmembers outlined in a certificate of inspection, vessels will often carry additional crew or industrial personnel with their own devices, and many vessels will contain OT systems with unique IP addresses. Although this comment is focused on U.S.-flagged vessels, it is evident that these same concerns could apply to estimated costs in the population of facilities and OCS facilities.

Based on these comments, the Coast Guard revisited its initial estimates and, in order to better estimate the costs associated with penetration testing, doubled the initial cost estimate to $10,000 and the estimate of the cost per IP address to $100, which better reflects industry averages.[121] In addition, to better estimate number of IP addresses on a given company's network, we now

[121] In 2023, RSI Security estimated that on average, a high quality, professional penetration test can cost from $10,000–$30,000, depending on the size, complexity, methodology, and scope of the test, among other factors. Our estimated range of $24,800 for owners and operators of facilities or OCS facilities, and $12,600 to $27,000 for most owners of one U.S.-flagged vessel, depending on the type of vessel, fall within this estimated range. Costs can exceed this range when considering owners of multiple vessels, or our estimated costs for the owner of the MODU in our population ($84,400, see section *Total Costs of the Final Rule per Affected Owner or Operator* in this RA for more details on this outlier vessel) given the additional network complexity we would expect to see based on the size of the organization and number of employees using its IT and OT systems. See *https://blog.rsisecurity.com/what-is-the-average-cost-of-penetration-testing/* for more information on industry estimates and factors contributing to penetration testing costs, accessed November 5, 2024.

use the number of employees and multiply it by 2 to capture employees potentially using multiple devices, additional industrial personnel working at facilities, or any OT systems on the network. We acknowledge that some owners or operators could face costs in excess of these estimates because of the large range of costs and network complexity, but our SMEs with penetration testing experience believe these adjustments better reflect average costs.

The number of employees for each facility is 74, meaning we estimate 148 IP addresses per owner or operator of a facility or OCS facility. Owners and operators of facilities and OCS facilities will incur penetration testing costs in conjunction with submitting and renewing the Cybersecurity Plan, or every 5 years. This means costs for penetration testing will be incurred in the second and seventh year of analysis. We estimate the undiscounted second- and seventh-year costs to owners and operators of facilities and OCS facilities for penetration testing to be about $10,887,200 [(439 facility owners and operators × $10,000) + (148 IP addresses × 439 facility owners and operators × $100)]. We estimate the discounted cost for owners and operators of facilities and OCS facilities to conduct penetration testing to be about $19,942,400 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be about $2,220,118 using a 2-percent discount rate. Using the same rate of baseline activity estimated for the overall population of facilities, we estimate that the subset of 3 owners or operators of OCS facilities will incur costs of $136,281 over a 10-year period of analysis and $15,172 annualized, using a 2-percent discount rate. See table 27.

Table 27: Estimated Costs of the Final Rule for Penetration Testing for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Number of Facility Owners and Operators	Number of IP Addresses per Owner and Operator	Initial Cost of Penetration Test	Cost per IP Address	Total Cost	2 Percent
1	0	0	$0	$0	$0	$0
2	439	148	$10,000	$100	$10,887,200	$10,464,437
3	0	0	$0	$0	$0	$0
4	0	0	$0	$0	$0	$0
5	0	0	$0	$0	$0	$0
6	0	0	$0	$0	$0	$0
7	439	148	$10,000	$100	$10,887,200	$9,477,963
8	0	0	$0	$0	$0	$0
9	0	0	$0	$0	$0	$0
10	0	0	$0	$0	$0	$0
Total					**$21,774,400**	**$19,942,400**
Annualized						**$2,220,118**

Note: Totals may not sum due to independent rounding.

Owners and operators of U.S.-flagged vessels will also need to conduct penetration testing, similar to facilities and OCS 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. Instead, we assume they will request waivers for these provisions, a cost included in Cybersecurity Plan development costs estimated earlier in the analysis. All estimates for penetration testing on U.S.-flagged vessels 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 $43,810,000 [(1,686 vessel owners and operators × $10,000) + (number of vessels for each vessel type × number of IP addresses for each vessel type × $100)]. See table 28 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, or $16,860,000 (1,686 owners and operators × $10,000) in Years 2 and 7.

Table 28: Estimated Costs of the Final Rule for Penetration Testing per IP Address for U.S.-flagged Vessels by Vessel Type (2022 Dollars, Undiscounted)

Vessel Type	Number of Vessels	Number of IP Addresses per Vessel	Cost per IP Address	Total for Population
MODU	1	744	$100	$74,400
Subchapter I Vessels	398	164	$100	$6,527,200
OSVs	430	32	$100	$1,376,000
Subchapter H Passenger Vessels	131	170	$100	$2,227,000
Subchapter K Passenger Vessels	430	70	$100	$3,010,000
Subchapter M Towing Vessels	4822	26	$100	$12,537,200
Subchapter D and Combination O&D Tank Vessels	114	80	$100	$912,000
Subchapters K and T International Passenger Vessels	53	54	$100	$286,200
Total				**$26,950,000**

Note: Totals may not sum due to independent rounding.

We estimate the discounted cost for owners and operators of U.S.-flagged vessels to conduct penetration testing to be approximately $80,248,045 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $8,933,736 using a 2-percent discount rate. See table 29.

Table 29: Estimated Costs of the Final Rule for Penetration Testing for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Total Cost	2 Percent
1	$0	$0
2	$43,810,000	$42,108,804
3	$0	$0
4	$0	$0
5	$0	$0
6	$0	$0
7	$43,810,000	$38,139,241
8	$0	$0
9	$0	$0
10	$0	$0
Total	**$87,620,000**	**$80,248,045**
Annualized		**$8,933,736**

Note: Totals may not sum due to independent rounding.

We estimate the total discounted cost to conduct penetration testing for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to be approximately $100,190,445 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $11,153,854 using a 2-percent discount rate. See table 30.

Table 30: Estimated Costs of the Final Rule for Penetration Testing for U.S.-flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Facilities and OCS Facilities Cost	U.S.-flagged Vessel Cost	Total Cost	2 Percent
1	$0	$0	$0	$0
2	$10,887,200	$43,810,000	$54,697,200	$52,573,241
3	$0	$0	$0	$0
4	$0	$0	$0	$0
5	$0	$0	$0	$0
6	$0	$0	$0	$0
7	$10,887,200	$43,810,000	$54,697,200	$47,617,204
8	$0	$0	$0	$0
9	$0	$0	$0	$0
10	$0	$0	$0	$0
Total	**$21,774,400**	**$87,620,000**	**$109,394,400**	**$100,190,445**
Annualized				**$11,153,854**

Note: Totals may not sum due to independent rounding.

Routine System Maintenance for Risk Management

The final cost provision under cybersecurity measures will be routine system maintenance for risk management, in § 101.650(e)(3)(i) through (vi). This final rule will require the CySO of a U.S.-flagged vessel, facility, or OCS facility to (1) ensure patching (software updates) or implementing controls for all KEVs in critical IT and OT systems in paragraph (e)(3)(i), (2) maintain a method to receive or act on publicly submitted vulnerabilities in paragraph (e)(3)(ii), (3) maintain a method to share threat and vulnerability information with external stakeholders in paragraph (e)(3)(iii), (4) ensure there are no exploitable channels exposed to internet accessible systems in paragraph (e)(3)(iv), (5) ensure that no OT is connected to the publicly accessible internet unless explicitly required for operation in paragraph (e)(3)(v), and (6) 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 RA, 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 to be patched 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 patching of OT systems, network segmentation, and uncertainty more in later sections in this final rule.

Based on information from CGCYBER, the cost for each owner or operator of a U.S.-flagged vessel, facility, and OCS facility to acquire third-party software capable of vulnerability scans will be approximately $3,390 annually, including the cost for a software subscription. 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 will 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 owners and operators of facilities and OCS facilities to subscribe to and use vulnerability scanning software to be approximately $4,651,0800 (1,372 facility owners and operators × $3,390). We estimate the undiscounted annual cost for the subset of 33 facilities owned and operated by 9 unique operators to subscribe to and use vulnerability scanning software to be approximately $30,510 (9 OCS facility owners and operators × $3,390) of the total cost estimate for facilities. We estimate the undiscounted annual cost for owners and operators of U.S.-flagged vessels to subscribe to and use vulnerability scanning software to be approximately $5,715,540 (1,686 vessel owners and operators × $3,390).

Combined, we estimate the total discounted cost for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to use vulnerability scanning software to be approximately $93,119,046 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $10,366,620, using a 2-percent discount rate. See table 31.

Table 31: Estimated Costs of the Final Rule for Vulnerability Scanning Software for U.S.-flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Facility and OCS Facility Costs	U.S.-flagged Vessel Costs	Total Cost	2 Percent
1	$4,651,080	$5,715,540	$10,366,620	$10,163,353
2	$4,651,080	$5,715,540	$10,366,620	$9,964,072
3	$4,651,080	$5,715,540	$10,366,620	$9,768,698
4	$4,651,080	$5,715,540	$10,366,620	$9,577,154
5	$4,651,080	$5,715,540	$10,366,620	$9,389,367
6	$4,651,080	$5,715,540	$10,366,620	$9,205,262
7	$4,651,080	$5,715,540	$10,366,620	$9,024,767
8	$4,651,080	$5,715,540	$10,366,620	$8,847,810
9	$4,651,080	$5,715,540	$10,366,620	$8,674,324
10	$4,651,080	$5,715,540	$10,366,620	$8,504,239
Total			$103,666,200	**$93,119,046**
Annualized				**$10,366,620**

Note: Totals may not sum due to independent rounding.

Total Costs of the Final Rule to Industry

We estimate the total discounted cost of this final rule to the affected population of facilities and OCS facilities to be approximately $514,932,875 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $57,325,689, using a 2-percent discount rate. See table 32.

As a subset of the cost estimate for facilities, we estimate that the 33 OCS facilities operated by 9 different owners and operators will incur costs of approximately $3,749,921 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized costs for OCS facilities to be approximately $417,466, using a 2-percent discount rate. See table 33.

BILLING CODE 9110–04–P

Table 32: Summary of Total Discounted Costs of the Final Rule for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-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	Total Costs	2 Percent
1	$15,641,626	$27,998,349	$4,785,771	$4,767,810	$0	$4,651,080	$57,844,636	$56,710,427
2	$17,206,630	$27,998,349	$2,688,771	$4,767,810	$10,887,200	$4,651,080	$68,199,840	$65,551,557
3	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$52,532,243
4	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$51,502,199
5	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$50,492,352
6	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$49,502,305
7	$4,927,238	$27,998,349	$2,688,771	$4,767,810	$10,887,200	$4,651,080	$55,920,448	$48,682,115
8	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$47,580,071
9	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$46,647,128
10	$15,641,626	$27,998,349	$2,688,771	$4,767,810	$0	$4,651,080	$55,747,636	$45,732,478
Total	**$147,266,876**	**$279,983,490**	**$28,984,710**	**$47,678,100**	**$21,774,400**	**$46,510,800**	**$572,198,376**	**$514,932,875**
Annualized							**$57,219,838**	**$57,325,689**
Percent of Total	25.74%	48.93%	5.07%	8.33%	3.81%	8.13%	100.00%	-

Note: Totals may not sum due to independent rounding

Table 33: Summary of Total Discounted Costs of the Final Rule for OCS Facilities as a Subset of the Total Costs for Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-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	Total Costs	2 Percent
1	$138,831	$183,663	$40,776	$32,434	$0	$30,510	$426,214	$417,857
2	$151,452	$183,663	$22,776	$32,434	$74,400	$30,510	$495,235	$476,004
3	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$384,669
4	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$377,127
5	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$369,732
6	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$362,482
7	$43,542	$183,663	$22,776	$32,434	$74,400	$30,510	$387,325	$337,190
8	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$348,407
9	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$341,575
10	$138,831	$183,663	$22,776	$32,434	$0	$30,510	$408,214	$334,878
Total	**$1,305,642**	**$1,836,630**	**$245,760**	**$324,340**	**$148,800**	**$305,100**	**$4,166,272**	**$3,749,921**
Annualized							**$416,627**	**$417,466**
Percent of Total	31.34%	44.08%	5.90%	7.78%	3.57%	7.32%	100.00%	-

Note: Totals may not sum due to independent rounding

BILLING CODE 9110–04–C

As seen in table 32, the primary cost drivers for the population of facilities and OCS facilities are costs for drills and exercises at 48.93 percent of the

total costs to industry. Cybersecurity Plan-related costs and costs for training come in second and third at 25.74 percent and 8.33 percent of the total costs, respectively. We believe some of this is due to the analysis of drills and exercises, and Cybersecurity Plan costs, which assume 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 measures 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 final rule to the affected population of U.S.-flagged vessels to be approximately $693,173,722 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $77,168,624, using a 2-percent discount rate. See table 34.

BILLING CODE 9110–04–P

Table 34: Summary of Total Costs of the Final Rule for U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-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	Total Costs	2 Percent
1	$6,983,620	$25,251,906	$36,357,096	$6,873,814	$0	$5,715,540	$81,181,976	$79,590,173
2	$7,683,665	$25,251,906	$21,183,096	$6,873,814	$43,810,000	$5,715,540	$110,518,021	$106,226,472
3	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$63,516,954
4	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$62,271,524
5	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$61,050,514
6	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$59,853,445
7	$2,200,093	$25,251,906	$21,183,096	$6,873,814	$43,810,000	$5,715,540	$105,034,449	$91,438,809
8	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$57,529,262
9	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$56,401,238
10	$8,380,344	$25,251,906	$21,183,096	$6,873,814	$0	$5,715,540	$67,404,700	$55,295,331
Total	**$75,529,786**	**$252,519,060**	**$227,004,960**	**$68,738,140**	**$87,620,000**	**$57,155,400**	**$768,567,346**	**$693,173,722**
Annualized							**$76,856,735**	**$77,168,624**
Percent of Total	9.83%	32.86%	29.54%	8.94%	11.40%	7.44%	100.00%	-

Note: Totals may not sum due to independent rounding.

BILLING CODE 9110–04–C

As in table 34, the primary cost drivers for the population of U.S.-flagged vessels are costs related to drills and exercises at 32.86 percent of the

total costs to industry. Costs related to account security measures and multifactor authentication come in second at 29.54 percent of the total costs. Costs related to penetration testing are third at 11.40 percent of the total costs. We estimate that costs for account security measures and multifactor authentication 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 population required to implement and manage multifactor authentication. In the NPRM, the Coast Guard requested public comment on who in the affected population of U.S.-flagged vessels has already implemented multifactor authentication and what the associated costs were but received no additional information.

We estimate the total discounted cost of this final rule to industry to be approximately $1,208,106,595 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $134,494,313, using a 2-percent discount rate. See table 35.

BILLING CODE 9110–04–P

BILLING CODE 9110–04–C

Table 35: Summary of Total Costs of the Final Rule to Industry (2022 Dollars, 10-year Discounted Costs, 2-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	Total Costs	2 Percent
1	$22,625,246	$53,250,255	$41,142,867	$11,641,624	$0	$10,366,620	$139,026,612	$136,300,600
2	$24,890,295	$53,250,255	$23,871,867	$11,641,624	$54,697,200	$10,366,620	$178,717,861	$171,778,029
3	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$116,049,197
4	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$113,773,722
5	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$111,542,865
6	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$109,355,750
7	$7,127,331	$53,250,255	$23,871,867	$11,641,624	$54,697,200	$10,366,620	$160,954,897	$140,120,924
8	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$105,109,333
9	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$103,048,366
10	$24,021,970	$53,250,255	$23,871,867	$11,641,624	$0	$10,366,620	$123,152,336	$101,027,809
Total	**$222,796,662**	**$532,502,550**	**$255,989,670**	**$116,416,240**	**$109,394,400**	**$103,666,200**	**$1,340,765,722**	**$1,208,106,595**
Annualized							**$134,076,572**	**$134,494,313**
Percent of Total	16.62%	39.72%	19.09%	8.68%	8.16%	7.73%	100.00%	-

Note: Totals may not sum due to independent rounding.

Total Costs of the Final 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 $50,362, under the assumption that an owner or operator will need to implement each of the provisions required by this final rule. Each additional facility owned or operated will 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 $73,320 for an owner or operator with one facility or OCS facility. See table 36 for a breakdown of the costs per entity for an owner or operator owning one facility or OCS facility.

Table 36: Summary of Total Costs of the Final Rule per Owner or Operator of a Facility or OCS Facility (2022 Dollars, 10-year Undiscounted Costs)[122]

Year	Facility Count	Cybersecurity Plan	Drills and Exercises	Account Security Measures	Multifactor Authentication	Cybersecurity Training	Penetration Testing	Vulnerability Management	Total
1	1	$4,207	$20,407	$576	$20,100	$4,633	$0	$3,390	$53,313
2	1	$8,414	$20,407	$576	$11,100	$4,633	$24,800	$3,390	$73,320
3	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
4	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
5	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
6	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
7	1	$1,893	$20,407	$576	$11,100	$4,633	$24,800	$3,390	$66,799
8	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
9	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
10	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
Total									**$503,623**
Annualized									**$50,362**

Note: Totals may not sum due to independent rounding.

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 will 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 will need to be resubmitted in the second year due to revisions that will 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 will need to be further revised and resubmitted in approximately 10 percent of cases as well. However, in this portion of the RA, 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 costs for each entity. 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 and operators will 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 37 displays the cost estimates per entity 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 37 by the number of owned facilities.

Table 37: Cybersecurity Plan-Related Costs of the Final Rule 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 costs for each entity for drills and exercises, account security measures, multifactor authentication, cybersecurity training, penetration testing, and vulnerability management.

For drills and exercises, we assume that a CySO on behalf of each owner and operator will develop cybersecurity drills and cybersecurity exercises. This development is expected to take 8 hours for each of the 2 annual drills and 20 hours for an annual exercise. We also include costs for drill and exercise participation for a portion of facility or OCS facility employees. We assume 33 percent of all employees will take 4 hours to participate in each drill and exercise, consistent with the share of shoreside employees estimated at U.S.-flagged vessel organizations. Using the loaded hourly wage for a CySO of

[122] The cost totals in table 36 represent cost estimates for owners and operators of one facility or OCS facility under the assumption that they will need to implement all cost-creating provisions of this final 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.

$84.14 and the loaded hourly wage for a facility employee of $60.34, we estimate annual costs of approximately $20,407 per facility owner or operator [($84.14 CySO wage × 8 hours × 2 drills) + ($84.14 CySO wage × 20 hours × 1 exercise) + (24 employees × $60.34 facility employee wage × 4 hours × 2 drills) + (24 employees × $60.34 facility employee wage × 4 hours × 1 exercise = $20,407], 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 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 36.

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)], as seen in table 36.

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 and OCS facilities will spend approximately $10,000 per penetration test and an additional $100 per IP address at the organization to capture network complexity. We use the total number of company employees multiplied by 2 as a proxy for the number of IP addresses, based on suggestions from public commenters stating that networks often include employees with multiple devices, outside industrial personnel accessing the networks, and OT systems that increase the number of IP addresses and the network complexity at a given company. As a result, we estimate second- and seventh-year costs of approximately $24,800 [$10,000 testing cost + ($100 × 148 IP addresses)], as seen in table 36.

For vulnerability management, we assume that each owner or operator of a 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 36.

We perform the same calculations to estimate the costs per entity 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 average annual costs for each entity of approximately $14,052 per U.S.-flagged vessel owner or operator, as seen in table 38.

Table 38: Summary of Costs of the Final Rule per Owner or Operator of U.S.-flagged Vessels (2022 Dollars, 10-year Undiscounted Costs)[123]

Year	Cybersecurity Plan	Drills and Exercises	Account Security Measures	Multifactor Authentication	Cybersecurity Training	Penetration Testing	Vulnerability Management	Total
1	$3,366	$3,029	$576	$9,000	$168	$0	$3,390	$19,529
2	$6,731	$3,029	$576	$0	$168	$10,000	$3,390	$23,894
3	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
4	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
5	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
6	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
7	$1,515	$3,029	$576	$0	$168	$10,000	$3,390	$18,678
8	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
9	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
10	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
Total								**$140,515**
Annualized								**$14,052**

Note: Totals may not sum due to independent rounding.

To estimate the costs that depend on the number and type of U.S.-flagged vessel for each entity, 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 39 displays the average number of employees for each vessel type, including shoreside employees, and their unique weighted mean hourly wages. Table 40 displays the per-vessel costs associated with each type of vessel.

Table 39: 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

[123] The cost estimates in table 38 represent the costs incurred at a company level for each owner and operator of U.S.-flagged vessels, so they must be added to the costs calculated in table 42, which are dependent on the type and number of vessels owned. We do this 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 this RA because we assume that each owner or operator will need to implement all provisions of this final rule that create costs. This is discussed in further detail in the analysis of costs per owner or operator.

Table 40: Summary of Annual Costs of the Final 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)[124]	Drills and Exercises	Total
MODU	1	$55,800	$14,731	$74,400	$43,718	$188,649
Subchapter I Vessels	1	$12,300	$3,802	$16,400	$11,126	$43,628
OSVs	1	$2,400	$879	$3,200	$2,636	$9,115
Subchapter H Passenger Vessels	1	$12,750	$3,557	$17,000	$10,546	$43,853
Subchapter K Passenger Vessels	1	$5,250	$1,593	$7,000	$4,916	$18,759
Subchapter M Towing Vessels	1	$1,950	$667	$2,600	$1,846	$7,063
Subchapter D and Combination O&D Tank Vessels	1	$6,000	$2,238	$8,000	$6,713	$22,951
Subchapter D, O, or I Barges	1	$0	$0	$0	$0	$0
Subchapters K and T International Passenger Vessels	1	$4,050	$1,204	$5,400	$3,746	$14,400

To calculate the total cost for each entity in the population of U.S.-flagged vessels, we add the annual per-vessel costs from table 40 based on the number and types of vessels owned to the per-entity costs estimated in table 38.

To estimate the cost for an owner or operator of a U.S.-flagged vessel to develop, resubmit, conduct annual maintenance for, and audit the Cybersecurity Plan, we use estimates provided earlier in this RA. 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 will 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 reviewers of Coast Guard VSPs at MSC, approximately 10 percent of Plans will need to be resubmitted in the second year due to revisions that will 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 will need to be further revised and resubmitted in approximately 10 percent of cases as well. However, in this portion of this RA, 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 costs for each entity.

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 will 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 41.

[124] When adding these costs to the per-entity costs for owners and operators, add only these estimated penetration costs in Years 2 and 7.

Table 41: Cybersecurity Plan-Related Costs of the Final Rule 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 costs for each entity for drills and exercises, account security measures, multifactor authentication, cybersecurity training, penetration testing, and vulnerability management.

For drills and exercises, we assume that, on behalf of each owner and operator, a CySO will develop new cybersecurity drills and cybersecurity exercises. This development is expected to take 8 hours for each of the 2 annual drills and 20 hours for an annual exercise. We also include costs for drill participation for a portion of U.S.-flagged vessel employees. We assume only shoreside employees will take 4 hours to participate in each drill and exercise. The costs per employee associated with drills and exercises vary depending on the types and number of vessels and will be based on the average number of shoreside 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 $54.92, we estimate annual drills and exercises costs of approximately $5,665 [($84.14 × 8 hours × 2 drills) + ($84.14 × 20 hours × 1 exercise) + ($54.92 × 4 average shoreside employees per OSV × 4 hours × 2 drills) + ($54.92 × 4 average shoreside employees per OSV × 4 hours × 1 exercise)]. Development costs per entity of $3,029 can be found in table 38 and variable per-vessel participation costs can be found in table 40.

For account security measures, we assume that, on behalf of each owner or operator, a database administrator 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 38.

For multifactor authentication, we assume that an owner or operator of a U.S.-flagged vessel 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 implementation costs of approximately $9,000 for all owners and operators, with annual costs in Years 2 through 10, depending 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). Implementation costs per entity of $9,000 for implementing the multifactor authentication system can be found in table 38, and variable costs per vessel can be found in table 40.

For cybersecurity training, we assume that on behalf of each owner or operator of a U.S.-flagged vessel, a CySO 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 costs per employee associated with training vary depending on the types and number of vessels and will 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 $54.92, we estimate annual training costs of approximately $1,047 [($84.14 × 2 hours) + ($54.92× 16 average employees per OSV × 1 hour)]. Development costs per entity of $168 can be found in table 38 and variable per vessel participation costs can be found in table 40.

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 U.S.-flagged vessels will spend approximately $10,000 per penetration test and an additional $100 per IP address at the organization to capture network complexity. We use the average number of employees per vessel multiplied by 2 as a proxy for the number of IP addresses, based on suggestions from

public commenters stating that networks often include employees with multiple devices, outside industrial personnel accessing the networks, and OT systems that increase the number of IP addresses and network complexity at a given company. As a result, we estimate second- and seventh-year costs as follows: [10,000 testing cost + ($100 × average number of employees per vessel)]. For example, we estimate second- and seventh-year cost of approximately $13,200 for an owner or operator of an OSV [$10,000 testing cost + ($100 × 32 average IP addresses per OSV)]. Initial costs of $10,000 per entity can be found in table 38, and variable per-vessel costs can be found in table 40.

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 38.

Unquantifiable Cost Provisions or No-Cost Provisions of This Final Rule

Communications

Under § 101.645, this final rule requires CySOs to have a method to effectively notify owners and operators of U.S.-flagged vessels, facilities, and OCS facilities, as well as personnel of changes in cybersecurity conditions. The requirements will 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 104.245 for vessels, 33 CFR 105.235 for facilities, and 33 CFR 106.240 for OCS facilities, the Coast Guard assumes that owners and operators of U.S.-flagged vessels, facilities, and OCS facilities already have communication channels established for physical security notifications which can easily be used for cybersecurity notifications. As a result, we do not estimate regulatory costs for communications. The Coast Guard received no public comments on this assumption and whether this communications provision will add an additional time burden.

Device Security Measures

Under § 101.650(b)(1), this final rule requires owners and operators of U.S.-flagged vessels, facilities, and OCS facilities 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 will be documented in the Cybersecurity Plan. Because this requirement is included in developing the Cybersecurity Plan, we estimated these costs earlier in that section of the cost analysis.

Under § 101.650(b)(2), this final rule requires owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to ensure applications running executable code are disabled by default on critical IT and OT systems. Based on information from CGCYBER, the time it will 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 provision.

Under § 101.650(b)(3) and (4), this final rule requires owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to develop and maintain an accurate inventory of network-connected systems, the network map, and OT device configuration. Because these items will be developed and documented as a part of the Cybersecurity Plan, we previously estimated these costs in that section of the cost analysis. The Coast Guard received several public comments on the NPRM related to its analysis of device security measures under this provision, stating that the Coast Guard underestimated costs. However, the Coast Guard received no additional information or cost-specific data that would allow us to adjust our estimates. As such, we retain our assumption that the 80 to 100 hours estimated for the overall Cybersecurity Plan development and maintenance are sufficient to capture the hour burdens associated with these device security measures like developing a network map or system inventory in addition to documenting policies and results related to measures like drills or training. As a result, our cost estimates are unchanged.

Data Security Measures

Under § 101.650(c), this final rule requires owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to securely capture, store, and protect logs, as well as use encryption to maintain confidentiality of sensitive data and integrity of IT and OT traffic, when technically feasible. The Jones Walker survey (see footnote number 60) reveals that 64 percent of 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 will need to comply with this final rule, or if data purchases will be necessary in all cases. The Coast Guard requested public comment on these estimates in order to update the analysis but received none. Therefore, we are unable to estimate regulatory costs for this provision.

Similarly, encryption is often available in default systems or in publicly available algorithms.[125] The Coast Guard will 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 will 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. Instead, in accordance with OMB Circular A–4, we include the storage and encryption of logs as source of uncertainty listed in table 42.

Routine System Maintenance

Under § 101.650(e)(3)(i) and (vi), owners and operators are required to patch KEVs in critical IT and OT systems (paragraph (e)(3)(i)) and conduct vulnerability scans (paragraph (e)(3)(vi)). The Coast Guard believes that these are processes that are typically

[125] For example, see the following web pages 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 August 22, 2024.

conducted in the background without much active work. However, we acknowledge the potential for these requirements to take additional time in certain circumstances, particularly when considering the complexity of patching and monitoring critical OT systems. Patching for IT systems can be set to automatically update and download without much risk, and vulnerability scans are typically background processes that need monitoring only in the event of an alert or incident. However, patching and monitoring of OT systems may be more complicated to allow for automatic updates and could even require periodically taking the systems offline. The Coast Guard lacks data on how prevalent critical OT systems are in the affected population, and how much time patching and monitoring could take in these unique systems.

While we received a public comment suggesting that we underestimated costs related to these provisions, we disagree with the commenter's suggestion that the provisions would require hiring additional employees, given our understanding of these processes as primarily occurring in the background.[126] As a result, without additional data on costs related to OT systems, we are unable to estimate costs for this provision, and instead include patching and monitoring of critical OT systems as a source of uncertainty listed in table 42.

Supply Chain Management

Under § 101.650(f)(1) and (2), this final rule includes provisions to specify measures for managing risks to the supply chain. This will not create any additional hour burden, as owners and operators will need to consider cybersecurity capabilities only 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 U.S.-flagged vessels, facilities, and OCS facilities of any cybersecurity vulnerabilities, incidents, or breaches that take place. Therefore, the Coast Guard does not estimate a cost for this provision.

Additionally, under § 101.650(f)(3), this final rule requires owners and operators of U.S.-flagged vessels, facilities, and OCS facilities 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 will need to document them only when developing the Cybersecurity Plan. We estimated these costs previously in the development of the Cybersecurity Plan section of this RA.

The Coast Guard requested public comment on the validity of this assumption and received several public comments stating that we underestimated costs, and that this requirement could require the hiring an additional employee. The Coast Guard acknowledges that this could take additional time, mostly through reviewing logs for remote connections, but we disagree that this would require a full-time employee, in most cases. The amount of time it takes is highly dependent on the size of the organization and its risk appetite, making accurate estimates difficult across organizations of various types and sizes, especially for those with simple networks and limited remote connections. As a result, we are unable to estimate costs for this provision, and instead include monitoring remote third-party connections as a source of uncertainty listed in table 42.

Resilience

Under § 101.650(g), each CySO for a U.S.-flagged vessel, facility, and OCS facility will be required to develop a Cyber Incident Response Plan, validate the effectiveness of Cybersecurity Plans through annual exercises or periodic reviews of incident response cases, and perform backups of critical IT and OT systems. In addition, entities not subject to 33 CFR 6.16–1 must report reportable cyber incidents to the NRC without delay. Of these requirements, the costs associated with developing a Cyber Incident Response Plan are already captured in the overall costs to develop the Cybersecurity Plan. Any subsequent annual maintenance for the Cyber Incident Response Plan will be captured in the costs for annual maintenance of the Cybersecurity Plan. In addition, costs associated with validating Cybersecurity Plans through annual exercises or periodic reviews of incident response cases is already captured in the costs estimated for drills and exercises in § 101.635.

For the population of entities not subject to 33 CFR 6.16–1 who must report reportable cyber incidents to the NRC without delay, we consider costs to be minimal, and do not include them in our total cost estimates. We base this decision on the removal of NRC reporting requirements for all U.S.-flagged vessels and facilities, as proposed in the NPRM. Now that reporting requirements only apply to entities not subject to 33 CFR 6.16–1, the only portion of the affected population subject to the new reporting requirements are the 33 OCS facilities affected by this final rule.

Based on historical cyber incident reporting data 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. However, OCS facilities only reported 1 cyber incident over that 5-year span. Although we anticipate that this number can increase or decrease following the publication of a final rule focused on cybersecurity standards and procedures, we use the historical averages to estimate costs for the affected population.[127] As a result, we estimate that OCS facilities only report 0.2 cyber incidents per year, on average. Using the methodology established in the NPRM, 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 ICR 1625–0096. This means that for the affected OCS facilities, we estimate annual undiscounted costs of $2.52 (0.2 cyber incident reports × 0.15 hours to report × $84.14 CySO wage). Given this low annual estimated cost, the Coast Guard does not include costs related to cyber incident reporting in its estimate of costs related to the final rule.

Further, the Coast Guard does not have data on the IT resources that

[126] Leading cybersecurity and vulnerability management firms like Qualys and Tenable produce vulnerability scanner technology that operates continuously in the background. In addition, Microsoft Defender (Microsoft's own vulnerability scanner for Windows, one of the most popular operating systems) has built-in and agentless scanners to continuously monitor and detect risk. See *https://learn.microsoft.com/en-us/defender-vulnerability-management/defender-vulnerability-management* for more details on how this scanner works in practice, accessed October 11, 2024.

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

owners and operators will 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.[128] The time burden of backing up data is minimal because backups can occur in the background through automated processes, making any new costs a result of making space for data storage. Providing external storage of data will require cloud storage (that is, storage on an external server), and the cost will be dependent upon the capacity needed; for example, 1 terabyte or 100 terabytes of space. These costs will likely be incurred on a monthly basis, although we do not know how much additional data space an owner or operator will 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. Instead, we consider these sources of uncertainty in table 42.

Network Segmentation

Under § 101.650(h)(1) and (2), this final rule requires owners and operators of U.S.-flagged vessels, facilities, and OCS facilities 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 U.S.-flagged vessels, facilities, and OCS facilities. 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 provision. The Coast Guard requested public comment on the anticipated costs of network segmentation within the affected population, especially from those who have previously segmented networks at their organizations. While we received several comments that stated we have underestimated costs related to network segmentation, we received no additional information that would have allowed us to adjust our analysis. Instead, in accordance with OMB Circular A–4, we include the storage and encryption of logs as source of uncertainty listed in table 42.

Physical Security

Under § 101.650(i)(1) and (2), this final rule will require owners and operators of U.S.-flagged vessels, facilities, and OCS facilities 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 final rule will impose new regulatory costs on owners and operators of U.S.-flagged vessels, facilities, and OCS facilities 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 requested but did not receive public comments on the anticipated costs associated with physical security provisions in this final rule above and beyond what has already been incurred under existing regulation. As such, we retain our assumption that this will not create additional costs, and leave costs associated with blocking, disabling, or removing of unused physical access ports on IT and OT infrastructure as a source of uncertainty in the analysis.

Hazardous Conditions

In addition to the requirements outlined in 33 CFR part 101, the Coast Guard is also amending the definition of a hazardous condition found in 33 CFR 160.202 to include ''cyber incident.'' This change impacts but does not create costs for the population of 11,222 U.S.-flagged vessels and the population of 11,490 foreign-flagged vessels that visit the U.S. each year on average.[129] Before this final rule, 33 CFR 160.202 defined a hazardous condition as ''any condition that may adversely affect the safety of any vessel, bridge, structure, or shore area or the environmental quality of any port, harbor, or navigable waterway of the United States. It may, but need not, involve collision, allision, fire, explosion, grounding, leaking, damage, injury or illness of a person aboard, or manning-shortage.'' The Coast Guard already interpreted this as including cyber incidents given the definition referring to ''any condition'' that ''may, but need not, involve,'' a list of potential conditions. This was never meant to be an exhaustive list, and, while the Coast Guard has previously interpreted it as including cyber incidents, we are now adding ''cyber incident'' to the list of example conditions to further clarify the affected population's obligation to report in light of this final rule. Accordingly, the Coast Guard does not estimate any costs related to this change.

Installation of Any New Software

Lastly, it is likely that this final rule will have unquantifiable costs associated with the incompatibility between the installation of the newer software and the use of older or legacy software systems on board U.S.-flagged vessels, facilities, and OCS facilities. We did not receive comments from the public on the anticipated costs associated with this difference in software for the affected population of this final rule, and instead include it as a source of uncertainty in table 42.

Sources of Uncertainty Related to Quantified Costs in the Rule

Given the large scope of this final rule, our analysis contains several areas of uncertainty that can lead us to overestimate or underestimate the quantified costs associated with certain provisions. In table 42, 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

[128] For example, the Ports and Terminals Cybersecurity Survey produced by Jones Walker referenced in footnote 60 asked facility owners and operators if their backups were ''segmented offline, cloud, redundant.'' Beyond this question appearing to assume that owners and operators are already conducting backups, 83 percent of respondents answered that their backups met the criteria, indicating that most owners and operators are conducting backups in this population.

[129] MISLE data indicates that, on average, 11,490 distinct foreign-flagged vessels entered the United States from 2021 through 2023 (11,346 in 2021, 11,717 in 2022, and 11,407 in 2023). Data was retrieved June 11, 2024. See table 6 in the *Affected Population* section of the analysis for more details on how the total of 11,222 U.S.-flagged vessels was calculated.

source of uncertainty ranked 2, and so on. The Coast Guard requested public comments from members of the affected populations of U.S.-flagged vessels, facilities, and OCS facilities who could provide insight into the areas of uncertainty specified in table 42, especially those relating to potential cost estimates, hour burdens, or current baseline activities. While we received several comments regarding underestimated costs, we did not receive information that allowed us to update our cost estimates for our sources of uncertainty.

BILLING CODE 9110–04–P

Table 42: Sources of Uncertainty in the Final 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 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	Not able to estimate.	1

Correction of vulnerabilities, performing fixes, and alleviating issues discovered in assessments, testing, or scanning	This final 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 final 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 rule. The costs associated with mitigations and vulnerability corrections will be highly dependent on what is discovered and will 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 § 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 U.S.-flagged vessels, facilities, and OCS facilities. 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 provision.	Underestimate	Not able to estimate.	4

§ 101.650(e)(3)(i) and (vi) - Patching and scanning for vulnerabilities in OT systems	The Coast Guard believes that patching of KEVs in critical IT and OT systems required under (i) and conducting vulnerability scans required under (vi) are processes that are typically conducted in the background without much active work. However, we acknowledge the potential for these requirements to take additional time in certain circumstances, particularly when considering the complexity of patching and monitoring critical OT systems. Patching for IT systems can be set to automatically update and download without much risk, and vulnerability scans are typically background processes that only need monitoring in the event of an alert or incident. Patching of OT systems may be more complicated to allow for automatic updates, but the Coast Guard lacks data on how prevalent these systems are in the affected population, and how much time this could take.	Underestimate	Not able to estimate.	5
§ 101.650(f)(3) - Monitoring and documenting all remote third-party connections	While we include costs for documenting remote third-party connections in the Cybersecurity Plan development and annual maintenance costs, we did not include a separate cost estimate for monitoring those connections under the assumption that the CySO would be aware of these remote connections as they would be specified in their existing contracts with third-party vendors. However, the Coast Guard acknowledges that this could take additional time, mostly through reviewing logs for remote connections.	Underestimate	Not able to estimate.	6

	The amount of time this could take is dependent on the size of the organization and its risk appetite, making accurate estimates difficult. As a result, we are unable to estimate costs for this provision.			
§ 101.665 Waivers and equivalency determinations	We acknowledge that it is likely there are other organizations beyond barge owners and operators with limited IT and OT systems who may request waivers under this rule. However, we are unable to determine who in the affected population will request waivers, and for which provisions, due to a lack of data. As a result, we are unable to estimate costs for this provision or determine where our other cost estimates may be overestimated. Costs for these organizations could be lower if they are able to secure a waiver rather than spend time or other resources to implement the required provisions.	Overestimate	Not able to estimate, but costs for drafting waiver requests could be included in the currently estimated Cybersecurity Plan development hours if the hour burdens to document the waived cybersecurity measures are reallocated.	7

§ 101.650(c) - Store logs and encrypt 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 will be the data space necessary to store the logs. The Coast Guard does not currently know who in the affected population will need to purchase additional data space to store logs, if any. Similarly, the Coast Guard does not know who in the affected population will need to purchase data encryption capabilities given a lack of information on systems in use that lack encryption capabilities.	Underestimate	The costs will 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.	8

§ 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 will be the data space necessary to store the data logs. The Coast Guard does not currently know who in the affected population will need to purchase additional data space to store logs, if any. Similarly, the Coast Guard does not know who in the affected population will 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 will 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.	9
§ 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 can 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. According to Coast Guard SMEs, costs for antitamper tape typically range from approximately $10 to $20 per 55-yard roll. Costs for access port	10

			locks range from approximately $10 to $20 for a pack of 10 locks. Costs for manually disabling ports on system hardware will 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 will 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 can be considered a no-cost provision of the rule.	11

BILLING CODE 9110–04–C

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 final 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 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.[130] Using these assumptions would result in estimated annual population costs of approximately $126,177 for account security ($970,596 primary estimated cost × 0.13), $6,015,705 for multifactor authentication implementation and maintenance ($35,386,500 primary estimated cost × 0.17), $5,155,361 for cybersecurity training ($6,873,814 primary estimate cost × 0.75), and $14,019,200 for penetration testing ($43,810,000 primary estimated cost × 0.32). This would result in reduced undiscounted annual cost estimates of approximately $61,724,467 for the population of U.S.-flagged vessels. See table 43.

Table 43: 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	$970,596	$126,177
Multifactor Authentication Costs	$35,386,500	$6,015,705
Cybersecurity Training Costs	$6,873,814	$5,155,361
Penetration Testing Costs	$43,810,000	$14,019,200
Total	**$87,040,910**	**$25,316,443**

The Coast Guard requested but did not receive public comments on whether these assumptions of baseline activity are more reasonable than what is currently used in this RA, 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. As such, we retained our assumption of no baseline activity in the affected population of U.S.-flagged vessels.

In addition, we considered adding cost estimates for those areas of uncertainty where we were able to estimate a range of potential costs. For provisions in § 101.650(c) and (g) related to storing 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 42, 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 because of this final rule, we would estimate approximately $510,384 ($372 × 1,372 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 final rule, we would estimate approximately $771,900 ($372 × 2,075 vessel owners and operators) in additional undiscounted annual costs to industry. See table 44.

[130] See footnote 60.

Table 44: Comparison of Cost Estimates for Alternative Data Space 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	$510,384	$5,103,840	$572,198,376	$577,302,216
U.S.-flagged Vessels	$771,900	$7,719,000	$768,567,346	$776,286,346
Total	**$1,282,284**	**$12,822,840**	**$1,340,765,722**	**$1,353,588,562**

These costs can change if we were to add additional assumptions about current baseline activities or adjusted the expected need for data space. We requested public comment on the accuracy and inclusion of these estimates but received none. As such, we were unable to add these cost estimates to our overall cost estimates for the rule.

Government Costs

There are two primary drivers of Government costs associated with this final rule. The first will be under § 101.630(d), where owners and operators of the affected population of U.S.-flagged vessels, facilities, and OCS facilities will 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, § 101.630(e) will 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 because of added Cybersecurity Plan components that will be reviewed as a part of an on-site inspection of U.S.-flagged vessels, facilities, and OCS facilities. An additional potential cost driver will be under § 101.650(g)(1), where owners and operators of the affected population of OCS facilities will be required to report cyber incidents to the NRC. The NRC will then need to process the report and generate notifications for each incident report they receive. However, based on historic NRC data related to cybersecurity incidents in the OCS facility population, we only estimate negligible costs related to this provision. 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 final 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 will 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 will 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 estimated hours to review initial, resubmitted, and renewal Cybersecurity Plans and amendments include review and approval of any requested waivers or equivalence determinations received from the affected owners and operators. 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 will submit Plans, which will be about 3,718 (33 of which are OCS facilities).

We determine the wage of a local facility inspector using publicly available data found in Commandant Instruction 7310.1W.[131] 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 facilities and OCS facilities to be approximately $13,500,944 [(3,718 facility Plan initial submissions × $89.00 × 40 hours) + (372 facility Plan resubmissions × $89.00 × 8 hours)]. Except in Year 7, when renewal of all Plans will occur, we estimate the undiscounted annual cost to the Coast Guard for the review of amendments to be approximately $1,323,608 (3,718 amendments × $89.00 × 4 hours). In Year 7, we estimate the undiscounted cost to be approximately $2,912,080 [(3,718 Plans for 5-year renewal × $89.00 × 8 hours) + (372 facility Plan resubmissions × $89.00 × 8 hours)]. We estimate the discounted cost for the Coast Guard to review U.S. facility and OCS facility Cybersecurity Plans to be approximately $23,679,103 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $2,636,112, using a 2-percent discount rate. See table 45.

BILLING CODE 9110–04–P

[131] 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 August 19, 2024.

Table 45: Estimated Final Rule Costs for Government to Review Facility and OCS Facility Cybersecurity Plans and Amendments (2022 Dollars, 10-year Discounted Costs, 2-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	2 Percent
1	$89.00	0	0	0	0	0	$0	$0
2	$89.00	3718	372	40	8	0	$13,500,944	$12,976,686
3	$89.00	3718	0	0	0	4	$1,323,608	$1,247,265
4	$89.00	3718	0	0	0	4	$1,323,608	$1,222,809
5	$89.00	3718	0	0	0	4	$1,323,608	$1,198,833
6	$89.00	3718	0	0	0	4	$1,323,608	$1,175,326
7	$89.00	3718	372	8	8	0	$2,912,080	$2,535,141
8	$89.00	3718	0	0	0	4	$1,323,608	$1,129,687
9	$89.00	3718	0	0	0	4	$1,323,608	$1,107,536
10	$89.00	3718	0	0	0	4	$1,323,608	$1,085,820
Total							**$25,678,280**	**$23,679,103**
Annualized								**$2,636,112**

Note: Totals may not sum due to independent rounding.

BILLING CODE 9110–04–C

Based on Coast Guard MSC estimates, it will 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 will 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 will submit Plans, about 2,075. 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.

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 $4,890,488 [(2,075 initial vessel Plan submissions × $81.83 × 28 hours) + (208 vessel Plan resubmissions × $81.83 × 8 hours)]. Except in Year 7, when resubmission of all Plans will occur, we estimate the undiscounted annual cost to the Coast Guard for reviewing amendments to be approximately $679,189 (2,075 amendments × $81.83 × 4 hours). In Year 7, we estimate the undiscounted cost to be approximately $1,494,543 [(2,075 Plans for 5-year renewal × $81.83 × 8 hours) + (208 vessel 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 $10,192,585 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $1,134,705, using a 2-percent discount rate. See table 46.

BILLING CODE 9110–04–P

Table 46: Estimated Final Rule Costs for Government to Review U.S.-flagged Vessel Cybersecurity Plans and Amendments (2022 Dollars, 10-year Discounted Costs, 2-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	2 Percent
1	$81.83	0	0	0	0	0	$0	$0
2	$81.83	2075	208	28	8	0	$4,890,488	$4,700,584
3	$81.83	2075	0	0	0	4	$679,189	$640,015
4	$81.83	2075	0	0	0	4	$679,189	$627,466
5	$81.83	2075	0	0	0	4	$679,189	$615,162
6	$81.83	2075	0	0	0	4	$679,189	$603,100
7	$81.83	2075	208	8	8	0	$1,494,543	$1,301,090
8	$81.83	2075	0	0	0	4	$679,189	$579,681
9	$81.83	2075	0	0	0	4	$679,189	$568,315
10	$81.83	2075	0	0	0	4	$679,189	$557,172
Total							**$11,139,354**	**$10,192,585**
Annualized								**$1,134,705**

Note: Totals may not sum due to independent rounding.

BILLING CODE 9110–04–C

The second source of Government costs is the marginal increase in onsite inspection time due to the expansion of FSPs, OCS FSPs, and VSPs to include

the Cybersecurity Plans and provisions by this final rule. The cybersecurity provisions will add to the expected onsite inspection times for the populations of U.S.-flagged vessels, facilities, and OCS facilities. 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 final rule will add an average of 1 hour to an onsite inspection, and that the inspection will 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.[132] Therefore, we estimate the annual undiscounted Government cost associated with the expected marginal increase in onsite inspections of facilities and OCS facilities is $267,696 (3,718 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 $2,404,602 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $267,696, using a 2-percent discount rate. See table 47.

Table 47: Estimated Final Rule Costs for Government for On-site Inspection of Facilities and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Number of Facilities	Facility Inspection Hours	Facility Inspector Wage	Total Cost	2 Percent
1	3718	1	$72	$267,696	$262,447
2	3718	1	$72	$267,696	$257,301
3	3718	1	$72	$267,696	$252,256
4	3718	1	$72	$267,696	$247,310
5	3718	1	$72	$267,696	$242,461
6	3718	1	$72	$267,696	$237,706
7	3718	1	$72	$267,696	$233,045
8	3718	1	$72	$267,696	$228,476
9	3718	1	$72	$267,696	$223,996
10	3718	1	$72	$267,696	$219,604
Total				**$2,676,960**	**$2,404,602**
Annualized					**$267,696**

Note: Totals may not sum due to independent rounding.

Similarly, Coast Guard SMEs within CG–ENG and inspectors in Coast Guard District 9 estimate that the additional cybersecurity provisions from this final rule will add an average of 0.167 hours (10 minutes) to an on-site inspection of a U.S.-flagged vessel and that the inspection will also 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. Therefore, we estimate the annual undiscounted Government cost associated with the expected marginal increase in onsite inspections of U.S.-flagged vessels is $108,696 (11,222 vessels × 0.167 hours inspection time × $72 vessel inspector wage). We estimate the total discounted cost of increased inspection time to be approximately $1,212,046 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $134,933, using a 2-percent discount rate. See table 48.

[132] 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 August 19, 2024.

Table 48: Estimated Final Rule Costs for Government for On-site Inspection of U.S.-flagged Vessels (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Number of Vessels	Vessel Inspection Hours	Vessel Inspector Wage	Total Cost	2 Percent
1	11222	0.167	$72	$134,933	$132,287
2	11222	0.167	$72	$134,933	$129,693
3	11222	0.167	$72	$134,933	$127,150
4	11222	0.167	$72	$134,933	$124,657
5	11222	0.167	$72	$134,933	$122,213
6	11222	0.167	$72	$134,933	$119,817
7	11222	0.167	$72	$134,933	$117,467
8	11222	0.167	$72	$134,933	$115,164
9	11222	0.167	$72	$134,933	$112,906
10	11222	0.167	$72	$134,933	$110,692
Total				**$1,349,330**	**$1,212,046**
Annualized					**$134,933**

Note: Totals may not sum due to independent rounding.

The final potential source of Government costs from this final rule is 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 0.2 cyber incident reports from OCS facilities per year. Cyber incident reports for other U.S.-flagged vessels and facilities are not included in this analysis because they are already required under 33 CFR 6.16–1. 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. However, because the rate of reportable cyber incidents in the population of OCS facilities is so low (only 0.2 reportable cyber incidents per year, on average), we estimate that any associated costs would be negligible. Therefore, we do not include cyber incident report processing costs in our estimated Government cost totals.

We estimate the total discounted Government costs of this rule for the review of Cybersecurity Plans and marginal increase in on-site inspection time to be approximately $37,488,336 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $4,173,446, using a 2-percent discount rate. See table 49.

Table 49: Total Estimated Costs of the Final Rule for Government (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rate)

Year	Facility Cybersecurity Plan Review Costs	Vessel Cybersecurity Plan Review Costs	Facility Inspection Costs	Vessel Inspection Costs	Total Cost	2 Percent
1	$0	$0	$267,696	$134,933	$402,629	$394,734
2	$13,500,944	$4,890,488	$267,696	$134,933	$18,794,061	$18,064,265
3	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$2,266,687
4	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$2,222,242
5	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$2,178,668
6	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$2,135,949
7	$2,912,080	$1,494,543	$267,696	$134,933	$4,809,252	$4,186,743
8	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$2,053,008
9	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$2,012,753
10	$1,323,608	$679,189	$267,696	$134,933	$2,405,426	$1,973,287
Total					**$40,843,924**	**$37,488,336**
Annualized					**$4,084,392**	**$4,173,446**

Note: Totals may not sum due to independent rounding.

Total Costs of the Rule

We estimate the total discounted costs of this final rule to industry and Government to be approximately $1,245,594,930 over a 10-year period of analysis, using a 2-percent discount rate. We estimate the annualized cost to be approximately $138,667,759, using a 2-percent discount rate. See table 50.

Table 50: Total Estimated Costs of the Final Rule to Industry and Government (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rates)

Year	Facility and OCS Facility Costs	U.S.-flagged Vessel Costs	Government Costs	Total Costs	2 Percent
1	$57,844,636	$81,181,976	$402,629	$139,429,241	$136,695,334
2	$68,199,840	$110,518,021	$18,794,061	$197,511,922	$189,842,293
3	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$118,315,883
4	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$115,995,964
5	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$113,721,533
6	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$111,491,699
7	$55,920,448	$105,034,449	$4,809,252	$165,764,149	$144,307,667
8	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$107,162,341
9	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$105,061,119
10	$55,747,636	$67,404,700	$2,405,426	$125,557,762	$103,001,097
Total	**$572,198,376**	**$768,567,346**	**$40,843,924**	**$1,381,609,646**	**$1,245,594,930**
Annualized				**$138,160,965**	**$138,667,759**

Note: Totals may not sum due to independent rounding.

Benefits

While the Coast Guard is able to describe the qualitative benefits that this final 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 final 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 final rule, both because the Coast Guard cannot quantify the effectiveness of the included provisions (how many attacks will be prevented or how much damage will 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 rule in terms of harms averted. We summarize public comments that highlight benefits of the final rule, provide a qualitative analysis of benefits, and analyze cyber incidents and risks addressed by the final rule below.

Public Comments That Support the Final Rule or Address Benefits

We received several public comments for the support of specific provisions of this final rule. For IT and OT systems, one commenter supports the requirements to ''designate critical IT and OT systems'' and to keep an inventory of these systems given the importance of an owner or operator knowing their own cybersecurity environment in order to properly defend it. Another commenter agrees ''that network segmentation is in fact an effective practice to help mitigate the damage caused by an attack on an IT or OT network.'' A third commenter ''strongly supports'' the ''requirements to analyze networks to identify IT and OT vulnerabilities, mitigate unresolved vulnerabilities, conduct vulnerability scans, and conduct annual penetration testing,'' because these provisions are key in ensuring resilience and preventing cybersecurity incidents.

We also received several comments about the use of and lack of reference to ASPs in the NPRM. Commenters recommended the Coast Guard to include the Cybersecurity Plan in existing ASPs. One commenter stated that submitting separate Cybersecurity Plans to the MSC for vessels and the local COTP for facilities is ''resource-intensive,'' and that ''the ASP framework has proved to be effective in allowing owners and operators to determine the best way to implement security requirements across the domestic passenger vessel fleet.'' The same commenter added, ''ASP should be added to applicable sections of the proposed rule when referencing requirements for FSP, VSP, or OCS FSP.'' Another commenter suggested permitting a Cybersecurity Plan to be included in an Alternative Security Program. This commenter stated that ''ASPs have been proven to be successful at both managing vessel and facility security risks and reducing costs and administrative burdens for vessel and facility operators, as well as the Coast Guard.''

Based on these comments, the Coast Guard revised § 101.660 of this final rule to explicitly allow owners and operators to use ASPs to comply with this final rule. We added additional text in § 101.660 to clarify that ASP provisions apply to cybersecurity compliance documentation. Given the unique nature of cybersecurity threats, vulnerabilities, and mitigation strategies, owners and operators must ensure that use of ASPs includes those items specific to each U.S.-flagged vessel, facility, and OCS facility. The Coast Guard will evaluate each ASP's cybersecurity component to ensure full regulatory compliance with each applicable requirement. These changes to this final rule can create marginal cost reductions and will create marginal benefits for owners and operators using ASPs because they are less resource intensive, as argued by several commenters. These owners and operators will not be required to submit separate Plans to the Coast Guard, and they will be able to include a Cybersecurity Plan as part of an approved ASP, which will allow owners and operators using ASPs to reallocate resources to implement or improve other cybersecurity measures.

We received numerous comments on the term ''reportable cyber incident.'' As a result, and as we stated in our response to comments in V. Discussion of Comments and Changes of this preamble, we included the use and definition of the term in this final rule, which will provide clear guidance on when and under what conditions cyber incidents must be reported to the NRC. This clarity will help eliminate the need to report minor cyber incidents, which will reduce the administrative burden on owners and operators.

We also received several public comments on the frequency of drills, with some requesting a general frequency reduction, others requesting annual or semi-annual drill requirements, and others requesting a schedule of requirements based on the cybersecurity risk faced by the affected U.S.-flagged vessels and facilities. These requests were made because commenters felt that the proposed quarterly drill requirements were too burdensome. As a result, the Coast Guard reduced the frequency of drills from quarterly to 2 drills in a calendar year. This will have a marginal benefit for affected owners and operators to use and direct resources to improve remaining drills or implement other cybersecurity measures that can help reduce the risk of a cyber incident in other ways.

Qualitative Analysis of 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.[133] In a paper published by Akpan, Bendiab, Shiaeles, Karamperidis, and Michaloliakos (2022), the authors state that the maritime sector has shown a 900-percent increase in cybersecurity

[133] 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 July 15, 2024.

breaches as it enters the digital era.[134] 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, GPS, and Global Navigation Satellite Systems. Other affected systems include radar systems; AIS; communication systems; and systems that control the main engine, generators, among others (Akpan et al., 2022).[135] Furthermore, the paper presents the vulnerabilities and consequences of cyber-attacks to ships' systems ranging from hijacking ships, destroying and stealing data, damaging equipment, disrupting vessel operations, uploading malware to computer systems, losing lives and cargo, and more (Akpan et al., 2022).[136]

In a paper by Jones (2016), the author noted that outdated systems are vulnerable to cyber-attacks. 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.[137]

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.[138] In a paper published by Meland, Bernsmed, Wille, Rodseth, and Nesheim (2021), the authors state that 46 successful [139] 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.[140] Some national governments have also used ransomware to advance their strategic interests, including evading sanctions.[141] The increased growth of cybercrime is a factor that has intensified in the last 20 years. Per the FBI's cybercrime reporting unit, financial losses from reported incidents of cybercrime exceeded $10.3 billion in 2022, and $35.9 billion from 2001 to 2022.[142] 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 exposed to risk.[143] In its 2018 report, the CEA stated, ''[b]ecause no single private entity faces the full costs of the adverse cyber events, the Government can step in to achieve the optimal level of cybersecurity, either through direct involvement or by incentivizing private firms to increase cyber protection.'' [144]

The overall benefit of this final rule is the reduction in the probability of a cyber incident and, if an incident occurs, improvement in the mitigation of its impacts. This benefits owners and operators and help protect the maritime industry and the United States. We expect this final rule to have significant but currently unquantifiable benefits for the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities, as well as downstream economic participants [145] and the public at large. This final rule benefits owners and operators of U.S.-flagged vessels, facilities, and OCS facilities by having a means, through the Cybersecurity Plan, to ensure that all cybersecurity measures are in place and tested periodically, which improves 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 final rule requires training, drills, and exercises, which benefits 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 also enables the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to prevent, detect, and respond to a cyber incident with improved capabilities.

In addition, cybersecurity measures in this final rule require owners and operators of U.S.-flagged vessels, facilities, and OCS facilities 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 physical requirements of this final rule ensure the minimal level of protection for critical IT and OT systems and allow for the proper monitoring of these systems. In table 51, we list the expected benefits associated with each major regulatory provision of this final rule.

BILLING CODE 9110–04–P

[134] 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;* accessed August 2024. Multidisciplinary Digital Publishing Institute 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 2024.

[135] Akpan et al., *supra* note 132, at 129–30.

[136] Id.

[137] Kevin Jones, ''Threats and Impacts in Maritime Cyber Security,'' April 15, 2016, pages 7 and 8, *https://www.researchgate.net/publication/304263412_Threats_and_Impacts_in_Maritime_Cyber_Security,* accessed August 15, 2024.

[138] 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,* accessed November 13, 2024. AGCS' website is *https://www.agcs.allianz.com.*

[139] 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, 2024.

[140] 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), accessed November 13, 2024. 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.

[141] 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 15, 2024.

[142] See the FBI'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 August 19, 2024. 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 August, 19, 2024.

[143] 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 15, 2024. See page 16 of the survey for data on industry confidence and pages 34–41 for data on cybersecurity practices.

[144] Economic Report of the President *supra* note 2 at 369.

[145] 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.

Table 51. Expected Actions of the Final 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."[146] 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 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."[147]
§ 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. This reduces 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 incidents more quickly, mitigating the impact of an attack and recovering quickly from cyber-attacks.
§ 101.650 Cybersecurity	1. Reduced risk of cyber-attacks: By ensuring that hardware and software components are genuine,

Measures. (f) *Supply chain.*	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."[148] Multiple authentication methods "may help to prevent cyber breaches across the supply chain,"[149] 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.[150] 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 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 can reduce the flow of commerce.

BILLING CODE 9110–04–C

Cyber Incidents and Risks Addressed by the Final Rule

In May 2021, a major pipeline company suffered a cyber-attack that disrupted the supply of fuel to the east coast of the United States. The 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 the 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.[151] Further, fuel shortages caused some fuel stations to temporarily close due to shortened supply. Some airlines in the impacted area were forced to scramble for additional fuel sources and added stops along select long-haul flights.[152] This was a ransomware cyber-attack that, based on public reports, was a result of the attackers using a legacy Virtual Private Network and the pipeline company not having a two-factor authentication method, more commonly known as multifactor authentication, in place on its computer systems.[153] Therefore, it was possible for computer hackers to access the pipeline company's computer systems with only a password.

This final rule can prevent an attack similar to the pipeline company 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 § 101.650.

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

Additionally, under § 101.650 for device security measures, documenting and identifying the network map and OT device configuration information, the pipeline company 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.

Lastly, the pipeline company did not have a Cybersecurity Plan in place but did have an emergency response plan. With § 101.630, Cybersecurity Plan, and § 101.635, Drills and Exercises, a Cybersecurity Plan could have benefitted the company 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 will 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 the pipeline company identify the issue of a weak password before it was exploited.

In another cyber-attack that occurred in 2017 against a major global shipping company, computer hackers, based on public reports, exploited the company's computer systems because of vulnerabilities in Microsoft's Windows operating system. The malware was disguised as ransomware, which created

[146] Economic Report of the President supra note 2 at 370.

[147] Economic Report of the President supra note 2 at 370 and 327.

[148] Economic Report of the President supra note 2 at 362.

[149] Economic Report of the President supra note 2 at 382–383.

[150] Economic Report of the President supra note 2 at 342.

[151] 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 August 15, 2024.

[152] 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 August 15, 2024.

[153] 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 August 15, 2024.

more damage to the company's computer systems. In 2016, one year before the attack, IT professionals at the shipping company highlighted imperfect patching policies, 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 the company 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 the company (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.[154] Under § 101.650, cybersecurity measures such as patching would likely prevent a similar attack from occurring and help prevent such losses. Patching U.S.-flagged vessel, facility, and OCS facility computer systems ensures they are not vulnerable to a cyber-attack because the latest software updates will be installed on these systems with periodic software patches.

Additionally, penetration testing may have identified the vulnerabilities in the shipping company's computer systems. Regular cybersecurity drills and exercises may have enabled the company's employees to quickly identify the cyber threat and may have reduced the impact and longevity of the cyber-attack. Further, network segmentation as 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, the shipping company 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 the company'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.[155] In this final rule, § 101.650 contains provisions for resilience, which owners and operators of companies such as this must possess to recover from a cyber-attack. With proper backups of critical IT and OT systems, this company may have been able to recover more quickly from the attack.

The Coast Guard emphasizes that this final rule might also have quantifiable benefits from reducing or preventing lost productivity from a cyber incident and possibly 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 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 can result in increases to commodity prices, while prolonged disruptions can 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 cybersecurity incident such as the attack that occurred against the global shipping company are difficult to quantify. They may include the effects of delays in cargo being delivered, which can result in the loss of some or all the cargo, especially if the cargo is comprised of perishable items such as food or raw goods; for example, certain types of oil that would be used later in the supply chain to manufacture final goods for consumption. Delays themselves may result in the unfulfillment of shipping orders to customers as vessels wait offshore to enter a port. This can create downstream effects for customers who would not receive goods because delivery trucks would sit idle at ports until OT and IT systems, either at the port or on board vessels, become operational again after the attack. Other societal impacts can include, but are not limited to, delays in shipments of medical supplies that may be carried on board vessels that would not be delivered on time to individuals and medical institutions relying on these supplies for their healthcare needs and service. 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 can 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 so on.

The benefits of this final rule can 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 this final rule's provisions prevented a terrorist or nation-state actor[156] 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.''[157] In addition, Ackerman and Heinzerling state ''terrorism 'works' through the fear and demoralization caused by uncontrollable uncertainty.''[158] As devastating as the direct impacts of a successful cyber-attack can be on the

[154] 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 August 15, 2024.

[155] 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 before 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 Ransomware Took Down Maersk,'' September 30, 2021, *https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/,* accessed August 15, 2024.

[156] 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 August 15, 2024) (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 (May 9, 2022), available at: *https://www.cisa.gov/uscert/ncas/alerts/aa22-110a,* accessed August 15, 2024.

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

[158] Frank Ackerman and Lisa Heinzerling, ''Priceless: On Knowing the Price of Everything and the Value of Nothing,'' 136–137 (2004).

U.S. MTS 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.

Through the provisions of this final 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 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 final rule addresses 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.

Analysis of Alternatives

The Coast Guard received multiple public comments regarding the penetration testing requirements that were the primary focus of our alternatives analysis in the NPRM. While we did receive a comment in support of the penetration testing requirement, many of the relevant comments highlighted concerns. Several commenters noted that penetration tests are expensive, and that the Coast Guard underestimated costs associated with the requirement. Further, some commenters stated that penetration tests would be ineffective at the frequency required in this final rule. In response, the Coast Guard revised our cost estimates to better reflect industry averages and continued to consider alternative frequencies of penetration testing in our analysis of alternatives. Despite the increased cost estimates, we ultimately decided to retain the proposed frequency of penetration testing, as analyzed below.

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 can threaten national stability. For instance, unauthorized access to a vessel's navigation system can 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 regulatory provisions in this final rule that identify potential network and system vulnerabilities. Of these provisions, penetration testing is one of the more intensive and costly, but provides important benefits, including demonstrating where and how malicious actors can 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 U.S.-flagged vessels, facilities, and OCS facilities 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 owners and operators of facilities and OCS facilities (see footnote number 60) and an unknown number of owners and operators of U.S.-flagged vessels 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 this final rule by $100,190,445, with an annualized cost reduction of $11,153,854 over a 10-year period of analysis, discounted at 2 percent, when compared to the preferred alternative. However, not requiring penetration testing would leave a significant gap in vulnerability detection capabilities 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 chose to require 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 costs approximately $10,000 per test, plus an additional $100 per IP address at the organization to capture network complexity. By increasing the frequency of these tests, the costs to U.S.-flagged vessels, facilities, and OCS facilities 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 $100,190,445 and annualized costs of $11,153,854 over a 10-year period of analysis, discounted at 2 percent (see the *Penetration Testing* section of the RA for more details on the calculations underlying this estimate). Requiring annual penetration testing would increase industry costs for penetration testing by just under 400 percent, to approximately $491,322,248 total and $54,697,200 annualized over a 10-year period of analysis, discounted at 2 percent. This alternative would result in a 31.4-percent increase in the total cost of this final rule, bringing the total cost to industry and the Government to approximately $1,636,726,735 total and $182,211,104, annualized, over a 10-year period of analysis, discounted at 2 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.

Table 52: Estimated Penetration Testing Costs of the Alternative for U.S.-flagged Vessels, Facilities, and OCS Facilities (2022 Dollars, 10-year Discounted Costs, 2-percent Discount Rates)

Year	Facilities and OCS Facilities Cost	U.S.-flagged Vessel Cost	Total Cost	2 Percent
1	$10,887,200	$43,810,000	$54,697,200	$53,624,706
2	$10,887,200	$43,810,000	$54,697,200	$52,573,241
3	$10,887,200	$43,810,000	$54,697,200	$51,542,393
4	$10,887,200	$43,810,000	$54,697,200	$50,531,758
5	$10,887,200	$43,810,000	$54,697,200	$49,540,939
6	$10,887,200	$43,810,000	$54,697,200	$48,569,548
7	$10,887,200	$43,810,000	$54,697,200	$47,617,204
8	$10,887,200	$43,810,000	$54,697,200	$46,683,534
9	$10,887,200	$43,810,000	$54,697,200	$45,768,170
10	$10,887,200	$43,810,000	$54,697,200	$44,870,755
Total	**$108,872,000**	**$438,100,000**	**$546,972,000**	**$491,322,248**
Annualized				**$54,697,200**

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 can hypothetically reduce costs for owners and operators for penetration testing down to zero, meaning a cost reduction of $100,190,445 and an annualized cost reduction of $11,153,854 over a 10-year period of analysis, discounted at 2 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 can 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 can be high, with potential downstream economic impacts, the Coast Guard must prioritize some level of oversight on provisions that can 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 § 101.665, owners and operators of U.S.-flagged vessels, facilities, and OCS facilities can seek a waiver or an equivalence determination, penetration testing included.

(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 (and ultimately chose) 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 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 can 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 can apply for waivers or equivalence determinations if they feel like they cannot meet the requirements related to penetration testing or find them unnecessary. According to § 101.665, an owner or operator, after completing the required Cybersecurity Assessment, may seek a waiver or an equivalence determination for any requirements in subpart F consistent with parallel waiver and equivalence provisions in 33 CFR parts 104, 105, and 106. If an owner or operator must temporarily deviate from the requirements, they must notify the cognizant COTP for facilities or OCS facilities, or the MSC for U.S.-flagged vessels, and may request temporary permission to continue to operate.

B. Small Entities

Under the Regulatory Flexibility Act (RFA), 5 U.S.C. 601–612, we have considered the impact of this final rule on small entities. The term ''small entities'' comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. The U.S. Small Business Administration (SBA) provides guidelines on the analytical process to assess the impact of a particular rulemaking on small entities.[159] With its proposed rule, the Coast Guard prepared and published an Initial Regulatory Flexibility Analysis (IRFA) because a threshold analysis indicated that the proposed rule may have a significant impact on a substantial number of small entities. After reviewing public comments, the Coast Guard's conclusion has not changed; it cannot certify the rule pursuant to the RFA. As a result, it is required to prepare a FRFA for publication with the final rule. A FRFA discussing the impact of this rule on small entities follows.

A FRFA addresses the following:

(1) A statement of the need for, and objectives of, the rule.

(2) A statement of the significant issues raised by public comments in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made in the proposed rule as a result of such comments.

(3) The response of the agency to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration in response to the proposed rule, and a detailed statement of any change made to the proposed rule in the final rule as a result of the comments.

(4) A description of and an estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available.

(5) A description of the projected reporting, recordkeeping, and other compliance requirements of the 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.

(6) A description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.

1. A statement of the need for, and objective of, the rule.

The maritime industry is undergoing a significant transformation that involves the increased use of cyber-connected systems. While these increasingly interconnected and networked 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. Cybersecurity threats require the maritime community to effectively manage constantly changing risks to create a safe cyber environment. Vulnerabilities in the operation of vital systems increase the risk of cyber-attacks. Unmitigated cyber-related risks to the maritime domain can compromise the critical infrastructure that people and companies depend on to fulfill their daily needs and that maintain the effective operation of the MTS.

A 2018 report by the CEA stated that ''[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.'' In the report, the CEA also emphasized the following:

''[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 research on cybersecurity, protecting critical infrastructures, preparing future employees for the cybersecurity workforce, and enforcing the rule of law in cyberspace.'' [160]

The objective of this final rule is to respond to the growing need for cybersecurity regulation in the MTS by establishing minimum performance-based cybersecurity requirements for U.S.-flagged vessels, facilities, and OCS facilities subject to MTSA. The 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. A statement of the significant issues raised by public comments in response to the IRFA, a statement of the assessment of the agency of such issues, and a statement of any changes made in the proposed rule as a result of such comments.

The Coast Guard did not receive any public comments specifically addressing the IRFA. However, it received several comments addressing costs experienced by regulated owners and operators of facilities and vessels, which affect estimates of per-entity costs, including the following:

[159] U.S. Small Business Administration (SBA). 2017. *A Guide for Government Agencies: How to Comply with the Regulatory Flexibility Act. https://advocacy.sba.gov/wp-content/uploads/2019/07/How-to-Comply-with-the-RFA-WEB.pdf*, accessed November 1, 2024.

[160] Economic Report of the President *supra* note 2 at 324–25.

• *Commenters stated that the cost estimates for penetration testing in the NPRM were underestimated.* In response to these comments, the Coast Guard adjusted its penetration testing cost estimates based on information provided by Coast Guard SMEs. The Coast Guard doubled the estimate of the initial penetration testing cost from $5,000 in the NPRM to $10,000 for the final rule, the cost per IP address from $50 in the NPRM to $100 for the final rule. In addition, the number of IP addresses per organization, which is now based on the number of employees in an organization, multiplied by 2.

• *Commenters raised concerns about the feasibility of combining cybersecurity and physical security drills and exercises and stated that we underestimated costs.* In its cost analysis, the Coast Guard now assumes that that no owners or operators will combine their cybersecurity drills with existing drills, and that all employees at the organization will participate in the new drills. Based on new information from Coast Guard SMEs in CG–FAC and LANTAREA, Coast Guard adjusted its cost estimates to reflect 8 hours for drill development and 4 hours for drill participation for vessel shoreside employees and the same share of facility and OCS facility employees. Based on this information, Coast Guard also adjusted its cost estimate for cybersecurity exercise development from 8 hours to 20 hours. To reduce the burden associated with the higher estimated cost of drills and exercises, the Coast Guard has reduced the frequency of required drills from quarterly to at least two drills every 12 months.

• Commenters noted a lack of reference to Alternative Security Programs (ASPs), and one commenter recommended that the Coast Guard amend § 101.630(a) to add ASPs to the requirement for CySOs. Some commenters specifically asked about using an ASP from the PVA, a trade association that represents several small entities. The Coast Guard will allow owners and operators to use ASPs to comply with this final rule. We added additional text to § 101.660 to clarify that ASP provisions apply to cybersecurity compliance documentation, giving small entities greater flexibility in how they can comply with the final rule. Given the unique nature of cybersecurity threats, vulnerabilities, and mitigation strategies, owners and operators must ensure that use of ASPs—including PVA's ASP, or ASPs developed on behalf of other small entities—contains those items specific to each U.S.-flagged vessel, facility, and OCS facility. The Coast Guard will evaluate each ASP's cybersecurity component to ensure full regulatory compliance with each applicable requirement.

• *Comments suggested that the affected population counts for U.S.-flagged vessels regulated under subchapters H and K used in the NPRM were inaccurate and provided updated numbers.* The Coast Guard updated its approach to counting the vessels that will be required to comply with this final rule. After including the public vessels, the Coast Guard finds that the population counts for U.S.-flagged vessels under subchapters K and H are approximately 430 and 131, respectively.

One commenter also stated that the regulation would create substantial costs for small entities in the commercial shipping sector. The Coast Guard has made waivers and equivalencies in § 101.665 available to affected owners and operators. These waivers offer additional flexibility to small entities, regardless of sector, that are not able to meet the full requirements. To further reduce the burden for impacted entities, the Coast Guard has opted for a delayed effective date of 180 days after the rule's publication in the **Federal Register**, extended the compliance deadline for the required Cybersecurity Assessment from 12 months to 24 months after the rule's effective date, and extended the compliance deadline for the Cybersecurity Plan from after the second annual audit of the existing physical security plan to 24 months after the rule's effective date. The Coast Guard is also requesting comment on a potential 2–5-year delay of the implementation periods for U.S.-flagged vessels and any potential costs or benefits the delay may have on small entities. However, beyond these changes to the implementation period and the reduction in cybersecurity drill frequency, the requirements of this final rule remain unchanged.

3. The response of the agency to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration in response to the proposed rule, and a detailed statement of any change made to the proposed rule in the final rule as a result of the comments.

The Chief Counsel for Advocacy of the SBA did not provide comment on the NPRM or the IRFA.

4. A description of and estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available.

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

Number of Small Entities Affected

As a first step, we identified the universe of affected owners and operators of U.S.-flagged vessels, facilities, and OCS facilities using information contained in the Coast Guard's MISLE database.[161] The affected population includes a mix of businesses, not-for-profit organizations, and governments. Because we applied a different method to determine which governments are small governments, the first step was to distinguish Government entities from all other entities in the affected population. To accomplish this, we searched on several keywords to identify and separate the universe of Government entities.[162] From the full population of affected owners (for profit, not-for-profit, and governments), we selected a random sample of U.S.-flagged vessel owners and a separate random sample of facility and OCS facility owners.[163]

For the sample of affected facility and vessel owners that are businesses and not-for-profit organizations, we identified which are likely to be small entities by matching business- and organization-specific information for a random sample with size standards for small businesses published in the SBA's Table of Small Business Size Standards.[164] [165] The SBA defines small

[161] The Coast Guard provided MISLE data to IEc on August 13, 2024.

[162] These keywords included: city, town, borough, state, commonwealth, district, authority, administration, municipality, department, army, port, division, and government. We visually inspect the results of the keyword searches to ensure that the identified entities are governments.

[163] Following the Coast Guard's recommended approach for drawing a random sample, we obtain sample sizes by applying two equations ($S = [(Z-2) \times p \times q] \div (e-2)$, and $S = N \div [1+(N \times (e-2))]$ where S is the sample size, Z=1.96, e= 0.05, p=0.5, q=0.5, and N = the number of vessel or facility owners in MISLE), and selecting the higher value obtained. We then apply random numbers between 0 and 1 to the unique owners identified in MISLE and select S number of owners with the highest random values. We perform this process separately for vessel owners and facility owners.

[164] U.S. Small Business Association (SBA). ''Table of size standards.'' Available at: *https://www.sba.gov/document/support-Table-size-standards* accessed November 14, 2024. Effective March 17, 2023.

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 owners of facilities and vessels. This analysis relied on the following steps:

(1) Upload the names and location information of the sampled entities to D&B Hoovers' website and rely on D&B Hoovers' proprietary algorithm to match entities with the information stored in its database; [166]

(2) Collect the primary NAICS code, ownership type,[167] number of employees,[168] and annual revenue information from entities that matched the information in D&B Hoovers' database;

(3) Determine which owners are small businesses and small not-for-profit organizations based on the SBA's definitions of small businesses matched to each NAICS code; [169] [170]

(4) Calculate the proportion of sampled businesses and not-for-profit organizations that are small entities; and

(5) Estimate the number of small businesses or small not-for-profit organization in the population by multiplying the sample proportions by the number of unique affected businesses and organizations in MISLE.

For the sample of government or quasi-governmental organization owners, we applied a different method to determine which are small. 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). The 2020 U.S. Census informed our classification of Government jurisdictions.[171]

Facility and OCS Facility Owners

Coast Guard identified 1,372 affected facility owners in MISLE.[172] Of these, a keyword search identified that 94 are Government entities and the remaining 1,278 are businesses and not-for-profit organizations. We generated a random sample of 384 affected owners, which included 37 of the affected governments also identified using the same keywords.[173] The names and location information of the owners in the sample were uploaded to D&B Hoovers. For the 347 business and not-for-profit organizations included in the sample, the search function returned information for 184 (53 percent) with at least 1 identified NAICS code.[174] Included among the owners that matched with records in D&B Hoovers were 181 businesses and 3 not-for-profit organizations. The 181 businesses categorize into 83 NAICS codes and 1 independent code used for ''Unclassified Establishments.'' [175]

Table 53 reports the number of businesses in the top 10 most frequently occurring classification codes (NAICS and the code for Unclassified Establishments) in the sample, as well as the portion that meet the definition of small business. An additional row summarizes the businesses across the remaining 74 NAICS codes. As presented, 155 of 181 businesses (86 percent) qualify as small based on their revenue or number of employees. Additionally, all 3 not-for-profit organizations are small organizations (100 percent). Under the assumption that all 163 facility owners in the sample for which D&B Hoovers profiles are not available are small businesses or organizations, we estimate that 321 of the 347 sampled facility owners are small entities (93 percent). Table 53 also presents findings for the governments. This analysis identifies that 11 of the 37 sampled government owners are small governments (30 percent).

Applying the percentage of affected small businesses and not-for-profit organizations identified in the sample (93 percent) to the total number of businesses and organizations identified in MISLE (1,278), we estimate that approximately 1,189 small businesses and small not-for-profit organizations may be directly affected by this final rule. Multiplying the percentage of affected small governments in the sample (30 percent) by the total number of governments identified with a keyword search of MISLE data (94), we estimate that approximately 28 small governments may be affected by this final rule. In total, 1,217 small entities that own facilities and OCS facilities may be affected by this final rule.

BILLING CODE 9110–04–P

---

[165] 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.

[166] 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 User Guide (2019, p. 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 September 2, 2024, accessed via: *https://app.dnbhoovers.com/login.*

[167] D&B Hoovers provides ownership type for the matched entities. For all entities not identified as governments using the keywords presented in footnote 160, this analysis considers all entities marked as ''private,'' ''public,'' or ''partnership'' as businesses. ''Nonprofit'' ownership status is used to identify not-for-profit organizations.

[168] 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.

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

[170] Revenue data contained in D&B Hoovers is presumed to be reported in 2023 dollars, aligned with the year preceding our download. This dollar year directly matches the year SBA last published its definitions of small businesses therefore we make no adjustments to the information from D&B Hoovers when comparing with SBA's reported thresholds.

[171] 2020 U.S. Census data accessed from: *https://www.census.gov/quickfacts/,* accessed October 21, 2024.

[172] Owners of facilities and OCS facilities are determined using various data fields in MISLE. Owner information is not reported in a standard format. Therefore, considerable data cleaning was necessary to identify unique owner names and location information. This analysis assumes that the sample of facilities with owner information identified is broadly representative of all regulated facility owners.

[173] The sample size of 384 is generated using the procedure described in footnote 161. Because OCS owners represent 1 percent of all facility owners in MISLE, we randomly selected 3 (1 percent of 384) OCS owners and 381 (99 percent of 384) facility owners from the unique owners identified in MISLE.

[174] Information for the identified governments were included in the D&B Hoovers search, but the D&B Hoovers output for these entities is not used in the analysis. Instead, government population data were manually obtained from the U.S. census.

[175] D&B Hoovers uses code 999990 for ''Unclassified Establishments.'' Because SBA does not provide a size standard for this code, we assume all entities with code 999990 are small. For the matched facilities owners, 5 entities are classified with this code in D&B Hoovers.

Table 53: Number and Portion of Small Entities in Random Sample Affected by the Final Rule's Requirements for Facilities and OCS Facilities

NAICS Code	Type of Industry	Size Standard Type	Size Standard (2023 Dollars)	Total Sampled Owners	Number of Sampled Owners Classified as Small	Percent Small
424720	Petroleum and Petroleum Products Merchant Wholesalers (except Bulk Stations and Terminals)	Number of employees	200	14	12	86%
488320	Marine Cargo Handling	Revenue	$47 million	9	9	100%
213112	Support Activities for Oil and Gas Operations	Revenue	$47 million	7	4	57%
336611	Ship Building and Repairing	Number of employees	1,300	7	7	100%
493190	Other Warehousing and Storage	Revenue	$36.5 million	6	5	83%
324110	Petroleum Refineries	Number of employees	1,500	6	6	100%
325211	Plastics Material and Resin Manufacturing	Number of employees	1,250	6	4	67%
483211	Inland Water Freight Transportation	Number of employees	1,050	5	5	100%
999990	Unclassified Establishments	Not available	Not available	5	5	100%
221118	Other Electric Power Generation	Number of employees	650	5	2	40%
74 Additional NAICS Codes	Various	Various	Various	111	96	86%
Matched Businesses	**Various**	**Various**	**Various**	**181**	**155**	**86%**
Matched Not-For-Profit Organizations	**Various**	**Various**	**Various**	**3**	**3**	**100%**
Unmatched Business and Organizations				**163**	**163**	**100%**

All Sampled Business and Not-for-Profit Organizations				**347**	**321**	**93%**
All Sampled Governments	**Public Sector**	**Population**	**50,000**	**37**	**11**	**30%**

Notes:

- The first 10 rows include the most frequently occurring classification 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.
- Code 999990 is used by D&B Hoovers to identify "Unclassified Establishments." All entities identified by code 999990 are assumed to be small.

BILLING CODE 9110–04–C

Vessel Owners

Across the categories of U.S.-flagged vessels regulated by the Coast Guard and considered for this rule, MISLE identifies over 10,000 vessels owned by 2,075 unique entities, including 72 government owners and 2,003 business and not-for-profit organization owners. We generated a random sample of 385 affected owners, which included 14 affected governments.[176] The names and location information in the sample were uploaded to D&B Hoovers. For the 371 business and not-for-profit organizations in the sample, the search function returned information for 249 owners (67 percent) with at least 1 identified NAICS code. Included among the owners that matched with records in D&B Hoovers were 244 businesses and 5 not-for-profit organizations. The 244 businesses categorize into 74 NAICS codes and 1 independent code used for ''Unclassified Establishments.[177]

Table 54 reports the number of businesses in the top 10 most frequently occurring classification codes (NAICS and the code for Unclassified Establishments) in the sample, as well as the portion that meet the definition of small business. An additional row summarizes the businesses across the remaining 65 NAICS codes. As presented, 228 of 244 businesses (93 percent) qualify as small based on their revenue or number of employees. Additionally, the 5 not-for-profit organizations include 4 small organizations (80 percent). Under the assumption that all 122 U.S.-flagged vessel owners in the sample for which D&B Hoovers profiles are not available are small entities, we estimate that 354 of the 371 sampled U.S.-flagged vessel owners (95 percent) are small businesses or small not-for-profit organizations. Table 54 additionally reports that our sample of 14 governments includes 2 small governments (14 percent).

Applying the percentage of affected small businesses and not-for-profit organizations identified in the sample (95 percent) to the total number of businesses and organizations identified in MISLE (2,003), we estimate that approximately 1,903 small businesses and small not-for-profit organizations may be directly affected by this final rule. Multiplying the percentage of affected small governments in the sample (14 percent) by the total number of governments identified with a keyword search of MISLE data (72), we estimate that approximately 10 small governments may be affected by this final rule. In total, 1,913 small U.S. entities that own U.S.-flagged vessels may be affected by this final rule.

BILLING CODE 9110–04–P

[176] The sample size of 385 is obtained by applying the procedure described in footnote 161 and including the one MODU owner identified in MISLE. To ensure that vessel owners of all affected types are represented in the sample, we sampled based on the distribution of owners by vessel type in MISLE: 211 Towing (55 percent of 384), 76 Barge (20 percent), 30 [U.S.-flagged passenger vessels subject to subchapter K] Pax K (8 percent), 25 OSV (7 percent), 21 Sub I (5 percent), 8 Tank (2 percent), 7 Pax H (2 percent), and 6 Pax International Travel (2 percent). Percentages do not sum to 100 due to rounding.

[177] D&B Hoovers uses code 999990 for ''Unclassified Establishments.'' Because SBA does not provide a size standard for this code, we assume all entities with code 999990 are small. For the matched vessel owners, 34 entities are classified with this code in D&B Hoovers.

Table 54: Number and Portion of Small Entities in Random Sample Affected by the Final Rule's Requirements for U.S.-flagged Vessels

NAICS Code	Type of Industry	Size Standard Type	Size Standard (2023 Dollars)	Total Sampled Owners	Number of Sampled Owners Classified as Small	Percent Small
999990	Unclassified Establishments	Not available	Not available	34	34	100%
488330	Navigational Services to Shipping	Revenue	$47 million	25	23	92%
237990	Other Heavy and Civil Engineering Construction	Revenue	$45 million	23	22	96%
483211	Inland Water Freight Transportation	Number of employees	1,050	9	9	100%
488999	All Other Support Activities for Transportation	Revenue	$25 million	8	8	100%
487210	Scenic and Sightseeing Transportation, Water	Revenue	$14 million	8	7	88%
424990	Other Miscellaneous Nondurable Goods Merchant Wholesalers	Number of employees	100	8	8	100%
483111	Deep Sea Freight Transportation	Number of employees	1,050	7	6	86%
483212	Inland Water Passenger Transportation	Number of employees	550	7	7	100%
532490	Other Commercial and Industrial Machinery and Equipment Rental and Leasing	Revenue	$40 million	6	5	83%
65 Additional NAICS Codes	Various	Various	Various	109	99	91%
Matched Businesses	**Various**	**Various**	**Various**	**244**	**228**	**93%**
Matched Not-For-Profit Organizations	**Various**	**Various**	**Various**	**5**	**4**	**80%**
Unmatched Businesses and Organizations				**122**	**122**	**100%**

All Sampled Businesses and Not-for-Profit Organizations					**371**	**354**	**95%**
All Sampled Governments	**Public Sector**	**Population**	**50,000**		**14**	**2**	**14%**

Notes:

- The first 10 rows include the most frequently occurring classification 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.
- Code 999990 is used by D&B Hoovers to identify "Unclassified Establishments." All entities identified by code 999990 are assumed to be small.

BILLING CODE 9110–04–C

Summary

Across the combined 3,447 affected owners of U.S.-flagged vessels, facilities, or OCS facilities, we estimate that 3,130 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 section compares the cost of the changes per U.S.-flagged vessel and facility 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.[178] For small governments, we use revenue information contained in publicly available annual financial reports for the year 2022. 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, 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.'' SBA also provides a list of options that can be used to determine whether an impact could be significant on a small entity, ''the impact could be significant if the cost of the proposed regulation (a) eliminates more than 10 percent of the businesses' profits; (b) exceeds 1 percent of the gross revenues of the entities in a particular sector or (c) exceeds 5 percent of the labor costs of the entities in the sector.'' [179] Therefore, this analysis considers the 1-percent threshold when analyzing these potential impacts.

Facility and OCS Facility Owners

Assuming that an operator would need to implement each of the provisions required by this final rule, the Coast Guard estimates that the highest single-year costs are incurred in Year 2 of the analysis period. We estimate that the Year 2 cost is $73,320 for an owner or operator with one facility. Each additional facility owned or operated would increase the estimated annual costs by the cost of an additional Cybersecurity Plan, since each facility will require an individual Cybersecurity Plan.[180] Table 55 provides a breakdown of the costs per owner or operator of one facility. The text that follows provides more detail on these cost calculations.

BILLING CODE 9110–04–P

[178] Revenue data from D&B Hoovers is presumed to be reported in 2023 dollars, the fiscal year preceding the year of download. We deflate these data to 2022 dollars to make the cost estimates using Gross Domestic Product reports from the Bureau of Economic Analysis, available at: *https://apps.bea.gov/iTable/?ReqID=19&step=4&isuri=1&1921=flatfiles.* See Table 1.1.9 of Section 1, accessed July 1, 2024.

[179] 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/.* Pages 18–19, accessed October 21, 2024.

[180] For example, consider an entity that owns four facilities. The estimated cost to that entity in Year 2 is calculated as follows: = $73,320 + (3 × $8,414) = $98,562.

Table 55: Summary of Total Costs of the Final 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	Total
1	1	$4,207	$20,407	$576	$20,100	$4,633	$0	$3,390	$53,313
2	1	$8,414	$20,407	$576	$11,100	$4,633	$24,800	$3,390	$73,320
3	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
4	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
5	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
6	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
7	1	$1,893	$20,407	$576	$11,100	$4,633	$24,800	$3,390	$66,799
8	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
9	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
10	1	$4,207	$20,407	$576	$11,100	$4,633	$0	$3,390	$44,313
Total									**$503,623**

Note: Totals may not sum due to independent rounding.

BILLING CODE 9110–04–C

To estimate the cost of the Cybersecurity Plan development, resubmission, annual maintenance, and audits for an individual facility or OCS facility owner or operator, we utilize the following estimates: 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 will 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 will 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 will 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 the development cost of 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 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 that owners will 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, 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**
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 will develop cybersecurity drills and cybersecurity components to add to existing exercises. This development is expected to take 8 hours for each of the 2 annual drills and 20 hours for an annual exercise. We also include costs for drill and exercise participation for facility or OCS facility employees. Because the Coast Guard is unable to determine which employees at a given facility or OCS facility will be in assigned cybersecurity duties and required to participate in the drills, we assume that 33 percent of all employees will participate. This share of employees is consistent with the estimated share of shoreside employees in the affected population of owners and operators of U.S.-flagged vessels. Coast Guard SMEs believe this is a more reasonable estimate than assuming the entire portion of employees will participate. We obtain the average number of facility employees from a Coast Guard contract that uses D&B Hoovers' database for company employee data. The average number of employees at a facility company is 74. We estimate that the average number of employees that will participate in cybersecurity drills is 24 (74 employees × 0.33). We assume that employees will take 4 hours to participate in each drill and 4 hours to participate in each exercise.

Using the loaded hourly wage for a CySO of $84.14 and the loaded hourly wage for a facility employee of $60.34, we estimate annual costs of approximately $20,407 per facility owner or operator [($84.14 CySO wage × 8 hours × 2 drills) + ($84.14 CySO wage × 20 hours × 1 exercise) + (24 employees × $60.34 facility employee wage × 4 hours × 2 drills) + (24 employees × $60.34 facility employee wage × 4 hours × 1 exercise) = $20,407] 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 a facility 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 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 will take 2 hours each year to develop and manage employee cybersecurity training, and facility employees 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)], 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 Cybersecurity Plan submission and renewal. We assume that facility owners and operators will spend approximately $10,000 per penetration test and an additional $100 per IP address at the organization in order to capture network complexity. We use the total number of company employees multiplied by 2 as a proxy for the number of IP addresses. This is based on suggestions from public commenters stating that networks often include employees with multiple devices, outside industrial personnel accessing the networks, and OT systems that increase the number of IP addresses and the network complexity at a given company. As a result, we estimate second- and seventh-year costs of approximately $24,800 [$10,000 testing cost + ($100 × 148 IP addresses)], as seen in table 55.

Finally, 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 55.

As demonstrated in table 55, affected entities are expected to incur the highest costs in Year 2 of this final rule. This analysis estimates the cost of the 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 the 332 presumed small entities in the sample (including those for which a D&B Hoovers profile was not matched, see table 53), 180 owners (54 percent) are associated with one facility ($73,320 cost in Year 2). The average small entity owns approximately 3 facilities, and the average cost across small entities is $90,148 in Year 2. The small entity in the sample with the highest projected cost owns 31 facilities ($325,740 cost in Year 2).

Table 57 compares the entity-specific Year 2 costs with the annual revenues of 131 small entities in our sample of affected facilities for which revenue information is provided in D&B Hoovers or obtained from 2022 annual financial reports (39 percent of the 332 small entities in our sample).[181] As shown, approximately 56 percent of small entities may incur costs that meet or exceed 1 percent of annual revenue in the second year of this final rule [(17 + 56) ÷ 131 = 56 percent]. The sampled small entity with the highest ratio of cost to revenue is projected to incur costs of 138 percent of its reported annual revenue, although it is possible that revenue data is underreported.

Table 17: Revenue Impact of the Final Rule on Sampled Small Entities Owning Facilities and OCS Facilities

% Revenue Impact	Greatest Annual Cost (Year 2)	
	Sampled Small Facility Owners with Known Revenue	Percentage of Sampled Small Facility Owners with Known Revenue
<1%	58	44%
1-3%	17	13%
>3%	56	43%
Total	**131**	**100%**

U.S.-Flagged 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 average annual costs per entity, regardless of the number of vessels owned and vessel type, in the first 10 years of rule implementation. The annual cost per entity ranges from $11,202 to $23,894. The data and assumptions underlying these estimates are provided later in this section.

BILLING CODE 9110–04–P

[181] Entity-specific Year 2 costs account for the number of facilities owned by the entity in question.

Table 58: Summary of Costs of this Final 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	Total
1	$3,366	$3,029	$576	$9,000	$168	$0	$3,390	$19,529
2	$6,731	$3,029	$576	$0	$168	$10,000	$3,390	$23,894
3	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
4	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
5	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
6	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
7	$1,515	$3,029	$576	$0	$168	$10,000	$3,390	$18,678
8	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
9	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
10	$4,039	$3,029	$576	$0	$168	$0	$3,390	$11,202
Total								**$140,515**

Note: Totals may not sum due to independent rounding.

BILLING CODE 9110–04–C

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 U.S.-flagged vessel type, as well as a unique weighted hourly wage based on the personnel employed on the U.S.-flagged vessels.[182] Table 59 displays the average number of employees for each U.S.-

[182] 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.''

flagged vessel type, including shoreside employees, and their unique weighted mean hourly wages. Table 60, which follows, displays the per-vessel costs associated with each type of U.S.-flagged vessel. To calculate the total cost per entity in the population of U.S.-flagged vessels, we add the annual per-vessel costs from table 60, multiplied by the number and types of U.S.-flagged vessels owned, to the per-entity costs presented in table 58.[183]

Table 59: Summary of Employees and Wages by Vessel Type

U.S.-flagged 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 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 Final 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)	Drills and Exercises	Total
MODU	1	$55,800	$14,731	$74,400	$43,718	$188,649
Subchapter I Vessels	1	$12,300	$3,802	$16,400	$11,126	$43,628
OSVs	1	$2,400	$879	$3,200	$2,636	$9,115
Subchapter H Passenger Vessels	1	$12,750	$3,557	$17,000	$10,546	$43,853
Subchapter K Passenger Vessels	1	$5,250	$1,593	$7,000	$4,916	$18,759
Subchapter M Towing Vessels	1	$1,950	$667	$2,600	$1,846	$7,063
Subchapter D and Combination O&D Tank Vessels	1	$6,000	$2,238	$8,000	$6,713	$22,951
Subchapter D, O, or I Barges	1	$0	$0	$0	$0	$0
Subchapters K and T International Passenger Vessels	1	$4,050	$1,204	$5,400	$3,746	$14,400

[183] For example, consider an entity that owns two subchapter H passenger vessels. The estimated cost to that entity in Year 2 is calculated as follows: (2 × $43,853) + $23,894 = $111,600.

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 will 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 will need to be resubmitted in the second year due to revisions that will 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), plans will 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 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 development cost of 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 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 that owners and operators will 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**
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 new cybersecurity drills and cybersecurity components to add to existing physical security exercises. This development is expected to take 8 hours for each of the 2 annual drills and 20 hours for an annual exercise. We also include costs for both drill and exercise participation for all U.S.-flagged vessel employees. We assume that employees will take 4 hours to participate in each drill and 4 hours to participate in each exercise.

Note that the per-employee costs associated with drills and exercises vary depending on the types and number of U.S.-flagged vessels. To determine the number of employees for each U.S.-flagged vessel company, we use data from the certificate of inspection manning requirements in MISLE for each vessel subpopulation. We assume 2 crews and multiply the total number of seafaring crew by 1.33 to account for shoreside staff to obtain an estimate of total company employees per vessel. We then subtract the total number of seafaring crew from the number of total company employees to arrive at the share of employees participating in the cybersecurity drills.[184] As an example, using the estimated CySO wage of $84.14 and the estimated OSV employee wage of $54.92, we estimate annual drills and exercises costs of

[184] For example, the average OSV in the affected population carries 12 seafaring crew per vessel, according to certificate of inspection manning requirements. We multiply this by 1.33 to arrive at 16 total employees per OSV. We then subtract the 12 seafaring crew from the 16 total employees to isolate the 4 shoreside employees per vessel that would need to participate in the cybersecurity drills.

approximately $5,665 [($84.14 × 8 hours × 2 drills) + ($84.14 × 20 hours × 1 exercise) + ($54.92 × 4 average employees per OSV × 4 hours × 2 drills) + ($54.92 × 4 average employees per OSV × 4 hours × 1 exercise)]. Development per-entity costs of $3,029 can be found in table 58, and variable per-vessel costs can be found in table 60.

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 58.

For multifactor authentication, we assume that a U.S.-flagged vessel owner or operator will spend $9,000 in the initial year on average to implement a multifactor authentication system and approximately $150 per employee annually for system maintenance and support. Therefore, we estimate first year implementation costs of approximately $9,000 for all owners and operators, with annual costs in Years 2 through 10 depending on the number of employees for each type of U.S.-flagged 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). 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 U.S.-flagged vessel owner or operator will take 2 hours each year to develop and manage employee cybersecurity training, and U.S.-flagged 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 U.S.-flagged vessels and will 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 $54.92, we estimate annual training costs of approximately $1,047 [($84.14 × 2 hours) + ($54.92 × 16 average employees per OSV × 1 hour)]. Development 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 U.S.-flagged vessel owners and operators will spend approximately $10,000 per penetration test and an additional $100 per IP address at the organization, to capture network complexity. We utilize the average number of employees per U.S.-flagged vessel multiplied by 2 as a proxy for the number of IP addresses. We do this based on suggestions from public commenters stating that networks often include employees with multiple devices, outside industrial personnel accessing the networks, and OT systems that increase the number of IP addresses and network complexity at a given company. As a result, we estimate second- and seventh-year costs as follows: [$10,000 testing cost + ($100 × average IP addresses per vessel)]. For example, we estimate second- and seventh-year cost of approximately $13,200 for an owner or operator of an OSV [$10,000 testing cost + ($100 × 32 average IP addresses per OSV)]. Initial per-entity costs of $10,000 can be found in table 58, and variable per-vessel costs can be found in table 60.

For vulnerability management, we assume that each 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 58. This analysis calculates U.S.-flagged vessel owner-specific annual compliance costs based on the type and number of vessels associated with each small entity in the sample. For the small entities that only own barges, there are no variable costs per vessel. We assume that they will incur only per-company costs related to the Cybersecurity Plan, as well as the development of and participation in drills and exercises. This means that the greatest per-owner costs occur in Year 2.

Our analysis identifies 67 small entities in the sample that fall into this category and presumes that this final rule will cost these entities $9,760 each in Year 2 ($6,731 Cybersecurity Plan related costs + $3,029 drills and exercises costs). For all other small entities that own U.S.-flagged vessels, the costs include a per-owner component as well as per-vessel costs that vary by vessel type. The highest total annual costs per owner also occur in Year 2. Among the 289 sampled small entities in this category, 164 owners (57 percent) are associated with one U.S.-flagged vessel (with an average cost of $38,229 in Year 2). The average small entity in the sample owns 3 U.S.-flagged vessels, and the average cost across all sampled small entities is $43,612 in Year 2. The small entity in the sample with the highest projected costs owns 8 U.S.-flagged vessels (with a cost of $299,214 in Year 2).

Table 62 compares the entity-specific costs in Year 2 with the greatest costs with the annual revenues of 222 small entities in our sample of affected U.S.-flagged vessel owners for which revenue information is provided in D&B Hoovers or through revenue information released by small governments (62 percent of 356 sampled small entities). As shown, 81 percent of small entities in the sample may incur costs that meet or exceed 1 percent of annual revenue in the second year of this final rule [(50 + 130) ÷ 222 = 81 percent]. After removing 1 significant outlier, the small entity in the sample with the highest ratio of cost to revenue is projected to incur costs of 131 percent of its reported annual revenue; although, it is possible that revenue data is underreported.

Table 62: Revenue Impact of the Final Rule on Small Entities Owning U.S.-flagged Vessels

% Revenue Impact	Greatest Annual Cost (Year 2)	
	Sampled Small Vessel Owners with Known Revenue	Percentage of Sampled Small Vessel Owners with Known Revenue
<1%	42	19%
1-3%	50	23%
>3%	130	59%
Total	**222**	**100%**

(*) Components may not add to total due to rounding.

Summary

The analysis above 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 and OCS facilities owned, according to data from the Coast Guard. We estimate that 56 percent of small facility and OCS facility owners and 81 percent of small U.S.-flagged vessel owners may incur costs that meet or exceed 1 percent of their annual revenue.

There are two reasons that the estimated compliance costs and, therefore, the impacts on small entities, are likely to be overestimated. First, the cost estimation approach assumes that all owners will incur costs associated with all provisions required in the rule. However, it is highly likely that many affected owners already have invested in some of the cybersecurity measures, absent the rule. Data available to the Coast Guard demonstrate this is the case for many facility owners, although whether those facility owners are small entities is uncertain. Second, some affected owners are unlikely to have IT or remotely accessible OT systems to which this final rule will apply. Those owners will only incur the cost associated with requesting a waiver or equivalence, costs which are likely to be far less than the costs described in this section.

5. A description of the projected reporting, recordkeeping, and other compliance requirements of the 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 rule will 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 VIII.D., Collection of Information, in the preamble of this final rule, includes 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 costs, please see the preceding analysis of the per-entity costs of the rule.

6. A description of the steps the agency has taken to minimize the significant economic impact of small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.

The purpose of this 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 has listed minimum performance-based cybersecurity requirements for the MTS. Like the existing requirements in 33 CFR parts 104, 105, and 106, the Coast Guard allows 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 FRFA represent conservative (upper-bound) estimates, as we attempt to capture costs for a wide range of affected owners and operators. Further, the Coast Guard has made waivers and equivalencies available to affected owners and operators who feel they are unable to meet the requirements of this rule, offering additional flexibility to small entities that are not able to meet the full requirements.

In addition to these intentional flexibilities, the Coast Guard made changes in response to public comments on the NPRM that will lessen the economic impact on all affected entities, including small entities. First, we reduced the required frequency of cybersecurity drills from quarterly to twice annually, reducing the overall effort expended on drills. In addition, the Coast Guard extended the implementation period and compliance dates for the cybersecurity requirements in this final rule beyond the 12 to 18 months that we proposed in the NPRM. We revised § 101.650(e)(1) to specify that owners and operators will need to conduct the Cybersecurity Assessment within 24 months of the effective date of this final rule. The Cybersecurity Plan must also be submitted to the Coast Guard for review and approval within 24 months of the effective date of this final rule, rather than during the second annual audit following the effective date, as stated in the NPRM. We revised § 101.655 to reflect this change. By using the same implementation period for each group of regulated entities rather than basing this on the

organization's audit date, the relevant owners and operators will have the same amount of time in which to implement these requirements, and in many cases will have additional time to come into compliance when compared to the NPRM.

Beyond the adopted changes and intentional flexibilities developed into this final rule, the Coast Guard also considered an alternative that would make the penetration testing requirements of this 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 $24,800 in the second and seventh years of analysis for an owner or operator of 1 facility or OCS facility. It would also lead to estimated cost reductions in the second and seventh years of $84,400 ($10,000 + $74,400) for owners and operators of a single MODU, $26,400 ($10,000 + $16,400) for owners and operators of a single U.S.-flagged vessel under subchapter I, $13,200 ($10,000 + $3,200) for owners and operators of a single OSV, $27,000 ($10,000 + $17,000) for owners and operators of a single passenger vessel under subchapter H, $17,000 ($10,000 + $7,000) for owners and operators of a single passenger vessel under subchapter K, $12,600 ($10,000 + $2,600) for owners and operators of a single towing vessel under subchapter M, $18,000 ($10,000 + $8,000) for owners and operators of a single tank vessel under subchapter D and a combination of subchapters O&D, and $15,400 ($10,000 + $5,400) for owners and operators of a single international passenger vessel 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 can 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 can 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 § 101.665, owners and operators of U.S.-flagged vessels, facilities, and OCS facilities can seek a waiver or an equivalence determination if they are unable to meet any requirements, penetration testing included.

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 rule so that they can better evaluate its effects on them and participate in the rulemaking. If the rule affects 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 rule. The Coast Guard will not retaliate against small entities that question or complain about this 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 rule calls 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 is new. The Coast Guard will collect information from the owners and operators of U.S.-flagged vessels, facilities, and OCS facilities under 33 CFR part 101, subpart F. The information collection will be for the submission of Cybersecurity Plans, amendments to Cybersecurity Plans in 33 CFR 101.630, and cyber incident reports in 33 CFR 101.650(g)(1).

Need for Information: The Coast Guard is creating new cybersecurity requirements for owners and operators of U.S.-flagged vessels, facilities, and OCS facilities to mitigate or prevent a cyber incident from occurring. The information we request from industry will be from (1) the development of Cybersecurity Plans, which will 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.

Use of Information: The Coast Guard will 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 Cybersecurity Plans and testing their IT and OT systems for adequacy. Additionally, the Coast Guard will 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, facilities, and OCS facilities.

Number of Respondents: The number of respondents will be about 2,075 U.S.-flagged vessel owners and operators and about 1,372 facility and OCS facility owners and operators. We assume that a CySO will be responsible for the reporting and recordkeeping requirements of the rule on behalf of each owner and operator.

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

Burden of Response: The burden of response will 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 will be about 268,900 hours across the affected population. This is derived from the development of 3,718 facility and OCS facility Cybersecurity Plans for 50 hours each and 2,075 vessel Cybersecurity Plans for 40 hours each [(3,718 × 50) + (2,075 × 40)]. For more information on how these and other burden estimates were developed, see the Regulatory Planning and Review section of this final rule.

For the second year of analysis, the hour burden for Cybersecurity Plan activities and cyber incident reporting will be about 295,820 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 3,718 facility and OCS facility Cybersecurity Plans for 50 hours each, 372 facility and OCS facility Cybersecurity Plans being revised and resubmitted for an additional 50 hours, 2,075 vessel Cybersecurity Plans for 40 hours each, and 208 vessel Cybersecurity Plans being revised and resubmitted for an additional 40 hours [(3,718 × 50) + (372 × 50) + (2,075 × 40) + (208 × 40)].

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 will be about 53,780 hours across the affected population. This is derived from the maintenance and amendment of 3,718 facility and OCS facility Cybersecurity Plans for 10 hours each, and the maintenance and amendment of 2,075 vessel Cybersecurity Plans for 8 hours each [(3,718 × 10) + (2,075 × 8)].

For the seventh year of analysis, when Cybersecurity Plans are renewed, the hour burden for Cybersecurity Plan activities and cyber incident reporting will be about 84,708 hours across the affected population. This is derived from the renewal of 3,718 facility and OCS facility Cybersecurity Plans for 15 hours each, 372 facility and OCS facility Cybersecurity Plans being revised and resubmitted for an additional 7.5 hours, 2,075 vessel Cybersecurity Plans being renewed for 12 hours each, and 208 vessel Cybersecurity Plans being revised and resubmitted for an additional 6 hours [(3,718 × 15) + (372 × 7.5) + (2,075 × 12) + (208 × 6)].

This leads to an average annual hour burden total of 102,589 hours over the 10-year period of analysis.

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

You need not respond to a collection of information unless it displays a currently valid control number from OMB. OMB has not yet completed its review of this collection. Once OMB completes action on our ICR, we will publish a **Federal Register** notice describing OMB's action.

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 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 final rule will 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 will 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.[185] Similarly, the cybersecurity requirements of this final rule as they apply to a facility under 33 CFR part 105 will 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 light of the foregoing analysis, this rule is consistent with the fundamental federalism principles and preemption requirements described in Executive Order 13132.

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 or where compliance with both a State and Federal laws is impossible or when a state law stands as an obstacle to the full purpose and objective of Congress, 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 rule will 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 Unfunded Mandates Reform Act of 1995addresses 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.

[185] 33 CFR 101.112(b).

After adjusting for inflation, this action will result in the expenditure of $176 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 117.973 and 66.939, respectively. We divide these values to obtain a factor of approximately 1.76, rounded (117.973 ÷ 66.939 = 1.76).[186] Multiplying this factor by the expenditure amount identified in the Unfunded Mandates Reform Act of 1995 gives us our expenditure amount adjusted for inflation (1.76 × 100,000,000 = 176,000,000). Because this rule will result in the expenditure by the private sector of approximately $178,717,861 in undiscounted 2022 dollars in the most cost-heavy year, this action requires an assessment. The RA, prepared in conjunction with this final rule, satisfies the Unfunded Mandates Reform Act of 1995's requirements under 2 U.S.C. 1532. In addition to the estimated impacts, it should be noted that many of the provisions in this rule are intentionally designed to take owner or operator discretion into account, which can help reduce anticipated expenditures. While this 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 final rule also includes the option for waivers and equivalents, in § 101.665, for any requirements in subpart F. 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 final rule will 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 final 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 analyzed this final rule under Executive Order 13045 (Protection of Children from Environmental Health Risks and Safety Risks). This final rule will not create an environmental risk to health or risk to safety that might disproportionately affect children.

J. Indian Tribal Governments

This final rule does not have Tribal implications under Executive Order 13175 (Consultation and Coordination with Indian Tribal Governments), because it will 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 final 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 will 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 final rule does not use technical standards. Therefore, we did not consider the use of voluntary consensus standards.

M. Environment

We have analyzed this final 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 determined 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 Record of Environmental Consideration supporting this determination is available in the docket. For instructions on locating the docket, see the **ADDRESSES** portion of this preamble.

This final rule is 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 final 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 final rule promotes the Coast Guard's maritime security mission by establishing measures to safeguard the MTS against emerging threats associated with cybersecurity. This final rule also promotes the Coast Guard's marine environmental protection mission by preventing or mitigating marine environmental damage that can ensue due to a cybersecurity incident.

N. Congressional Review Act

Pursuant to the Congressional Review Act (5 U.S.C. 801 *et seq.*), the Office of Information and Regulatory Affairs has determined that this final rule meets the criteria in 5 U.S.C. 804(2).

List of Subjects

33 CFR Part 101

Harbors, Maritime security, Reporting and recordkeeping requirements, Security measures, Waterways.

33 CFR Part 160

Administrative practice and procedure, Harbors, Hazardous materials transportation, Marine safety,

[186] 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#eyJhcHBpZCI6MTksInN0ZXBzIjpbMSwyLDMsM10sImRhdGEiOltbIk5JUEFfVGFibGVfTGlzdCIsIjEzIl0sWyJDYXRlZ29yaWVzIiwiU3VydmV5Il0sWyJGaXJzdF9ZZWFyIiwiMTk5NSJdLFsiTGFzdF9ZZWFyIiwiMjAyMyJdLFsiU2NhbGUiLCIwIl0sWyJTZXJpZXMiLCJBll1dfQ==,* accessed August 20, 2024.

Navigation (water), Personally identifiable information, Reporting and recordkeeping requirements, Seamen, Vessels, Waterways.

For the reasons discussed in the preamble, the Coast Guard amends 33 CFR parts 101 and 160 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; Executive Order 12656, 3 CFR, 1988 Comp., p. 585; 33 CFR 1.05–1, 6.04–11, 6.14, 6.16, and 6.19; Department of Homeland Security Delegation No. 00170.1, Revision No. 01.4.

■ 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 U.S.-flagged vessels, facilities, and Outer Continental Shelf (OCS) 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, facilities, and OCS facilities required to have a security plan under 33 CFR parts 104, 105, and 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 stored separately for preservation and recovery. 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 (IT) or Operational Technology (OT) system used by the vessel, facility, or OCS facility that, if compromised or exploited, could result in a transportation security incident (TSI), 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 TSI. 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 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 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. The owner or operator may designate an alternate CySO(s) to assist with the duties and responsibilities of the CySO, including during periods when the CySO is on leave, unavailable, or unable to perform their duties. Hereafter, ''CySO'' will refer to both the CySO and the alternate CySO(s), as applicable.

Cybersecurity Plan means a plan developed as a part of the VSP, FSP, or OCS FSP 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; as an annex to a VSP, FSP, or OCS FSP; provided in a separate submission from the VSP, FSP, or OCS FSP; or addressed through an Alternative Security Program.

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 IT, OT, 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.

Log means a record of the events occurring within an organization's systems and networks.

Multifactor authentication means a layered approach to securing data and applications for a system that requires users to present more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

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.

Reportable cyber incident means an incident that leads to or, if still under investigation, could reasonably lead to any of the following: Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system; 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 potential for significant impact on public health or safety or may cause serious injury or death; Disclosure or unauthorized access directly or indirectly of nonpublic personal information of a significant number of individuals; Other potential operational disruption to critical infrastructure systems or assets; or Incidents that otherwise may lead to a transportation security incident as defined in 33 CFR 101.105.

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: The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and 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 U.S.-flagged vessel, facility, or OCS facility is responsible for compliance with the requirements of this subpart.

(b) For each U.S.-flagged 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 Cybersecurity Officer (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 U.S.-flagged 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) For entities that have not reported to the Coast Guard pursuant to, or are not subject to, 33 CFR 6.16–1, ensure all reportable cyber incidents are reported to the National Response Center (NRC).

§ 101.625 Cybersecurity Officer.

(a) *Other duties.* The Cybersecurity Officer (CySO) may serve in other roles or positions and may perform other duties within the owner's or operator's organization (U.S.-flagged vessel, facility, or OCS 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 U.S.-flagged vessel, facility, or OCS facility. If a person serves as the CySO for more than one U.S.-flagged vessel, facility, or OCS facility, the name of each U.S.-flagged vessel, facility, or OCS facility for which that person is the CySO must be listed in the Cybersecurity Plan of each U.S.-flagged vessel, facility, or OCS facility for which that person is the CySO.

(c) *Assigning Duties Permitted.* The CySO may assign security duties to other U.S.-flagged vessel, facility, or OCS facility personnel; however, the CySO retains ultimate responsibility for these duties.

(d) *Responsibilities.* For each U.S.-flagged 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);

(6) Arrange for cybersecurity inspections, which may be conducted as their own inspections, or in conjunction with any scheduled Coast Guard inspection of a U.S.-flagged vessel, facility, or OCS facility;

(7) Ensure the prompt correction of problems identified by exercises, audits, or inspections;

(8) Enhance the cybersecurity awareness and vigilance of personnel;

(9) Ensure adequate cybersecurity training of personnel;

(10) Ensure all reportable 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;

(12) Ensure any reports as required by this part have been prepared and submitted;

(13) Ensure that the Cybersecurity Plan, as well as proposed amendments to cybersecurity measures included in the Plan, 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 U.S.-flagged vessels, prior to amending the Cybersecurity Plan, in accordance with § 101.630;

(14) Ensure relevant security and management personnel are briefed regarding changes in cybersecurity conditions on board the U.S.-flagged 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, education, 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 U.S.-flagged vessels, facilities, or OCS facilities. 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, FSP, or an OCS FSP; as an annex to the VSP, FSP, or OCS FSP; as part of an approved Alternative Security Program; or may be provided in a separate submission from the VSP, FSP, or OCS 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 a facility or OCS facility, or to the MSC for a U.S.-flagged vessel.

(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 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 may 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 U.S.-flagged vessels, facilities, or OCS facilities of similar operations must ensure the Plan addresses the specific cybersecurity risks for each U.S.-flagged vessel, facility, or OCS 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 submit its proposed amendments. Until the amendments are approved, the owner or operator must ensure temporary cybersecurity measures are implemented to the satisfaction of the Coast Guard.

(2) 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.

(i) Nothing in this section should be construed as limiting the owner or operator of the U.S.-flagged vessel, facility, or OCS facility from the timely implementation of such additional security measures not enumerated in the approved VSP, FSP, or OCS FSP as necessary to address exigent security situations.

(ii) In such cases, the owner or operator must notify the cognizant COTP for a facility or OCS facility, or the MSC for U.S.-flagged vessels, by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(3) If the owner or operator has changed, the CySO must amend the Cybersecurity Plan as soon as reasonably practicable in light of the individual circumstances, but, in any case, not longer than 96 hours, 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 as soon as reasonably practicable in light of the individual circumstances, but, in any case, not longer than 96 hours, 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 as soon as reasonably practicable in light of the individual circumstances, but, in any case, not longer than 96 hours.

(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 ensure that an audit of the Cybersecurity Plan occurs if there is a change in the owner or operator of the U.S.-flagged 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) Additional audits of the Cybersecurity Plan as a result of modifications to the U.S.-flagged vessel, facility, or OCS facility, or because of changes to the cybersecurity measures in accordance with paragraph (f)(2) of this section, 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 U.S.-flagged 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.

§ 101.635 Drills and exercises.

(a) *General.* (1) Drills and exercises must be used to test the proficiency of the U.S.-flagged 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 U.S.-flagged 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 cybersecurity drills are conducted at least twice each calendar year. Cybersecurity drills may be held in conjunction with other security or non-security drills, as required by 33 CFR 104.230, 105.220, or 106.225, 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 U.S.-flagged vessel, facility, or OCS facility; changes to the U.S.-flagged 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 as required by 33 CFR 104.230, 105.220, or 106.225; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be vessel-, facility-, or OCS 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 U.S.-flagged 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, reportable cyber 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 U.S.-flagged vessel, facility, or OCS facility of changes in cybersecurity conditions at the U.S.-flagged vessel, facility, and OCS facility and document these means in Section 5 of the Cybersecurity Plan.

(b) Communication systems and procedures must allow effective and continuous communications between U.S.-flagged 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 U.S.-flagged 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 systems;

(2) Default passwords must be changed before using any IT or OT systems. When changing default passwords is not feasible, appropriate compensating security controls must be implemented and documented;

(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. When multifactor authentication is not feasible, appropriate compensating security controls must be implemented and documented;

(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 U.S.-flagged vessel, facility, or OCS facility must ensure the following device security measures are in place, addressed in Section 6 of the Cybersecurity Plan, and made available to the Coast Guard upon request:

(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 are disabled by default on critical IT and OT systems;

(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 U.S.-flagged 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) Logs must be securely captured, stored, and protected so that they are accessible only by privileged users; and

(2) Effective encryption must be deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic, when technically feasible.

(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) When personnel must access IT or OT systems but are unable to receive cybersecurity training as specified in paragraphs (d)(1) and (2) of this section, they must be accompanied or monitored by a person who has completed the training specified in paragraphs (d)(1) and (2) of this section.

(4) All personnel must complete the training specified in paragraphs (d)(1)(ii) through (v) of this section by January 12, 2026, and annually thereafter. Key personnel must complete the training specified in paragraph (d)(2) of this section by January 12, 2026, 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 U.S.-flagged vessels, 105.225 for facilities, and 106.230 for OCS facilities.

(e) *Risk management.* Each owner or operator or designated CySO of a U.S.-flagged 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 U.S.-flagged vessel, facility, and OCS facility. A Cybersecurity Assessment must be conducted no later than July 16, 2027, 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. In conducting the Cybersecurity Assessment, the owner or operator must—

(i) Analyze all networks to identify vulnerabilities to critical IT and OT systems and the risk posed by each digital asset;

(ii) Validate the Cybersecurity Plan;

(iii) Document recommendations and resolutions in the Vessel Security Assessment (VSA), Facility Security Assessment (FSA), or OCS FSA, in accordance with 33 CFR 104.305, 105.305, and 106.305;

(iv) Document and ensure patching or implementing of documented compensating controls for all KEVs in critical IT or OT systems, without delay; 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).

(2) *Penetration testing.* In conjunction with Cybersecurity Plan renewal, the owner, operator, or designated CySO must ensure that a penetration test has been completed. Following the penetration test, a letter certifying that the test was conducted, as well as all identified vulnerabilities, must be included in the VSA, FSA, or OCS FSA, 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 U.S.-flagged 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 U.S.-flagged 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 or reportable cyber incidents, 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 U.S.-flagged 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) For entities that have not reported to the Coast Guard pursuant to, or not subject to, 33 CFR 6.16–1, report reportable cyber incidents to the NRC without delay;

(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 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 U.S.-flagged 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, operator, or designated CySO of a U.S.-flagged 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 no later than July 16, 2027, according to 33 CFR 104.410 for U.S.-flagged vessels, 33 CFR 105.410 for facilities, or 33 CFR 106.410 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 apply to cybersecurity compliance documentation and are addressed in 33 CFR 104.140 for vessels, 33 CFR 105.140 for facilities, and 33 CFR 106.135 for OCS facilities.

§ 101.665 Noncompliance, waivers, and equivalents.

An owner or operator, after completion of the required Cybersecurity Assessment, may seek a waiver or an equivalence determination for the requirements in subpart F using the standards and submission

procedures applicable to a U.S.-flagged vessel, facility, or OCS facility as outlined in 33 CFR 101.130, 104.130, 104.135, 105.130, 105.135, 106.125, or 106.130. If an owner or operator must temporarily deviate from the requirements in this part, they must notify the cognizant COTP for facilities or OCS facilities, or the MSC for U.S.-flagged vessels, 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.

PART 160—PORTS AND WATERWAYS SAFETY—GENERAL

■ 3. The authority citation for part 160 is revised to read as follows:

Authority: 46 U.S.C. 70001–70003, 70034, and Chapter 701; DHS Delegation 00170.1, Revision No. 01.4. Subpart C is also issued under the authority of 46 U.S.C. 3715 and 46 U.S.C. 70011.

■ 4. Amend § 160.202 by revising the definition for Hazardous condition to read as follows:

§ 160.202 Definitions.

* * * * *

Hazardous condition means any condition that may adversely affect the safety of any vessel, bridge, structure, or shore area or the environmental quality of any port, harbor, or navigable waterway of the United States. It may, but need not, involve collision, allision, fire, explosion, grounding, leaking, damage, cyber incident, injury or illness of a person aboard, or manning-shortage.

* * * * *

Dated: January 8, 2025.

Linda Fagan,

Admiral, U.S. Coast Guard, Commandant.

[FR Doc. 2025–00708 Filed 1–13–25; 4:15 pm]

BILLING CODE 9110–04–P