U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Via email: www.regulations.gov

May 22, 2024

Commander Brandon Link
Chief, Cyber and Critical Infrastructure Protection Branch
Office of Port and Facility Compliance
U.S. Coast Guard
Washington Navy Yard, DC 20374

Re: Notice of Proposed Rulemaking, Coast Guard, Department of Homeland Security (DHS); Cybersecurity in the Marine Transportation System (Docket No. USCG-2022-0802; 89 *Federal Register*, February 22, 2024)

Dear Commander Link:

The U.S. Chamber of Commerce welcomes the opportunity to comment on the Coast Guard's notice of proposed rulemaking (NPRM or the proposed rule) on Cybersecurity in the Marine Transportation System.[1] We also appreciate the additional time that was given to stakeholders to provide officials with feedback.

This proposed rule would apply to the owners/operators of U.S.-flagged vessels subject to 33 CFR part 104, facilities subject to 33 CFR part 105, and Outer Continental Shelf (OCS) facilities subject to 33 CFR part 106. The proposed requirements include account security measures, device security measures, data security measures, governance and training, risk management, supply chain management, resilience, network segmentation, reporting, and physical security.[2]

The Chamber does not cover every element of the NPRM. Instead, our comments generally urge the Coast Guard to prioritize the following actions and policies:

- Advancing regulatory harmonization, such as between elements of the Coast Guard's proposed rule and the Transportation Security Administration's (TSA's) pipeline security directives.

[1] https://www.federalregister.gov/d/2024-03075
https://www.federalregister.gov/d/2024-07512

[2] https://www.federalregister.gov/d/2024-03075/p-110

- Making the requirements of the NPRM more performance based and less prescriptive. Performance-based approaches enhance security by stipulating that critical security outcomes are achieved while allowing owners/operators to choose the most appropriate security measures for their specific systems and operations.[3]

- Aligning cyber incident reporting under the NPRM with the Cybersecurity and Infrastructure Security Agency's (CISA's) proposed rule related to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[4]

I. HARMONIZATION

The Chamber believes that protecting key critical infrastructure from malign cyber activity is an economic and national security priority. For several years, federal, state, and local governments and industry have embraced a partnership model to defend critical infrastructure from nation-states and criminal hacking outfits. This approach has largely been successful.

The Chamber has concerns with the proliferation of cybersecurity laws, regulations, and guidance documents at the state, federal, and international levels. Although it is a significant actor, the Coast Guard is one of many governmental bodies that is promulgating broad and detailed cybersecurity regulations impacting industry and maritime entities in particular.

Nonetheless, the Coast Guard's NPRM provides authorities with an opportunity to make progress in harmonizing some of the multiple cybersecurity rules that businesses must comply with—and the list continues to increase. Here is a case in point: Some industry entities operate thousands of miles of interstate natural gas pipelines and multiple liquified natural gas (LNG) facilities, which serve as essential links between natural gas producers and consumers. The security of interstate natural gas pipelines is regulated by TSA under the Aviation and Transportation Security Act; the security of LNG import and export terminals is regulated by the Coast Guard under the Marine Transportation Security Act of 2002 (MTSA).

Owing to the integrated nature of information systems at LNG facilities, including having many of the connections regulated under TSA directives (e.g., because of the potential for remote access to pipeline networks), there is a significant overlap in regulatory authority for cybersecurity at these facilities. The Chamber urges the Coast Guard to harmonize duplicative requirements between its proposed rule and TSA's July 2023 security directive on *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (TSA security directive).

In our letter, the Chamber points to elements of the NPRM and comparable parts of the TSA security directive (note the bulleted points in dark blue), which should be considered candidates for regulatory harmonization.

---

[3] For example, see DHS, "Ratification of Security Directives," *Federal Register* (*FR*), April 19, 2024, p. 28571.

[4] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

§ 101.620—Owner/Operator (*FR*, pp. 13410, 13510)

Among other things, this section would require each owner/operator of a covered entity—that is, a vessel, facility, or OCS facility—to assign appropriate personnel to develop a Cybersecurity Plan and ensure that it incorporates detailed preparation, prevention, and response activities for cybersecurity threats and vulnerabilities.[5]

- Section III.F.2 of the 2023 TSA security directive already requires assigning personnel to manage cybersecurity matters associated with information technology (IT) and operational technology (OT).[6]

§ 101.630—Cybersecurity Plan (*FR*, pp. 13410, 13510)

This section would set minimum requirements for an organization's Cybersecurity Plan, which would incorporate the results of a Cybersecurity Assessment and appropriate protective measures. Also, the format of a Cybersecurity Plan would include some 14 individual sections.[7]

- Section I, paragraph 5.1–3 of the TSA security directive already calls for establishing and implementing a series of plans (i.e., assessment, implementation, and incident response) consistent with the Coast Guard's proposed Cybersecurity Plan. For example, owners/operators must create and maintain a Cybersecurity Incident Response Plan to reduce the risk of operational disruption. Moreover, section 1 calls for owners/operators to develop a Cybersecurity Assessment Plan each year and submit it to TSA for approval.[8]

§ 101.635—Drills and Exercises (*FR*, pp. 13411, 13511)

Under this section, cybersecurity drills and exercises would be required to test the proficiency of a covered entity's personnel in assigned cybersecurity duties, including the implementation of the Vessel Security Plan (VSP), Facility Security Plan (FSP), OCS FSP, and Cybersecurity Plan. The NPRM adds that drills and exercises would also enable the Cybersecurity Officer (CySO) to identify any related cybersecurity deficiencies that need to be addressed.[9]

Cybersecurity drills would generally test one or more elements of a Cybersecurity Plan. A drill would be required *at least once every three months* and could be held in conjunction with

---

[5] https://www.federalregister.gov/d/2024-03075/p-219

[6] TSA, Security Directives and Emergency Amendments. https://www.tsa.gov/sd-and-ea

TSA, Security Directive Pipeline-2021-02D: *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* (TSA security directive), July 26, 2023, pp. 8–9. https://www.tsa.gov/sites/default/files/tsa-sd-pipeline-2021-02d-w-memo_07_27_2023.pdf

[7] https://www.federalregister.gov/d/2024-03075/p-229

[8] TSA security directive, pp. 1–2.

[9] https://www.federalregister.gov/d/2024-03075/p-253

other drills. The Coast Guard says that cybersecurity exercises are a full test of an organization's cybersecurity regime and would include substantial and active participation of cybersecurity personnel. The exercises would be required at least once each calendar year, with no more than 18 months between exercises.[10]

- Section III.F of the TSA security directive already requires a number of exercises to test an owner's/operator's Incident Response Plan.[11]

§ 101.640—Records and Documentation (*FR*, pp. 13411, 13512)

This section would require owners/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. The Coast Guard notes that records must be kept for at least two years and be made available to officials upon request. The records, the Coast Guard adds, could be kept in paper or electronic format and must be protected against unauthorized access, deletion, destruction, amendment, and disclosure.

Also, records that each covered entity keep would vary because each organization would maintain records specific to its operations. At a minimum, the records would have to capture the following activities: training, drills, exercises, cybersecurity threats, incidents, and audits of the Cybersecurity Plan as set forth in the cited recordkeeping requirements above and made applicable to records under this subpart per section 101.640.[12]

- Facility records and documents are already maintained per the Coast Guard's facility recordkeeping requirements under 33 CFR 105.225.[13] In addition, sections IV.A through IV.C of the TSA security directive contain specific requirements on recordkeeping to, among other things, establish an owner's/operator's compliance with the directive.[14]

§ 101.645—Communications (*FR*, pp. 13411, 13512)

This section would require a CySO to maintain an effective means of communication to convey changes in cybersecurity conditions to the personnel of a covered entity. A CySO would be called on to maintain an effective and continuous means of communicating with security personnel, U.S.-flagged vessels interfacing with the facility or OCS facility, the captain of the port, and national and local authorities who have responsibilities regarding security.[15]

---

[10] https://www.federalregister.gov/d/2024-03075/p-254
https://www.federalregister.gov/d/2024-03075/p-255

[11] TSA security directive, pp. 8–9.

[12] https://www.federalregister.gov/d/2024-03075/p-258

[13] https://www.law.cornell.edu/cfr/text/33/105.225

[14] TSA security directive, pp. 10–11.

[15] https://www.federalregister.gov/d/2024-03075/p-259

- Communication requirements are already defined in section III.F of the TSA security directive, which pertain to having a Cybersecurity Incident Response Plan. Security Directive Pipeline—2021-01C calls for the Cybersecurity Coordinator to serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA.[16]

§ 101.650—Cybersecurity Measures (*FR*, pp. 13412, 13512)

§ 101.650 Paragraph (a): Account Security Measures

This section would impose on covered entities "minimum account measures to protect critical IT and OT systems from unauthorized cyber access and limit the risk of a cyber incident."[17]

- Section III.C of the TSA security directive already mandates that owners/operators implement access controls, among other account security measures.[18]

§ Section 101.650 Paragraph (b): Device Security Measures

This section would provide specific proposed requirements to mitigate risks and vulnerabilities in critical IT and OT systems and equipment. This paragraph would apply the "Identify" function of the NIST CSF.

- Section III.A of the TSA security directive already requires that owners/operators designate "Critical Cyber Systems," including devices, as well as maintain policies and controls to safeguard IT and OT systems.[19] Also, directive sections IV.C.2.a and IV.C.2.c already require owners/operators to undertake a network mapping and an inventory of their hardware and software.[20]

§ 101.650 Paragraph (c): Data Security Measures

This section would mandate "fundamental data security measures that stem from the 'Protect' function of the NIST CSF" and are consistent with basic risk management activities of the maritime industry.[21]

The Coast Guard notes that these measures would "establish baseline protections upon which owners/operators could build. This paragraph would require data logs to be securely captured, stored, and protected so that they are accessible only by privileged users, and would

---

[16] https://www.tsa.gov/sites/default/files/sd-pipeline-2021-01c.pdf, p. 2.

[17] https://www.federalregister.gov/d/2024-03075/p-262

[18] TSA security directive, pp. 5–6.

[19] Ibid., p. 5.

[20] Ibid., pp. 10–11.

[21] https://www.federalregister.gov/d/2024-03075/p-270

require encryption for data in transit and data at rest. CySOs would rely on generally accepted industry standards and risk management principles to determine the suitability of specific encryption algorithms for certain purposes, such as protecting critical IT and OT data with a more robust algorithm than for routine data." Further, "A CySO would establish more detailed data security policies in section 9 of a Cybersecurity Plan. Those policies would be adapted to the unique operations of the U.S.-flagged vessel, facility, or OCS facility."[22]

- The security of data in transit is already required by section III.B.2.b of the TSA security directive. Operational data within the OT is not encrypted. IT data encryption is typically determined by corporate policy.[23]

§ 101.650 Paragraph (d): Cybersecurity Training for Personnel

- Cybersecurity training is often required by the corporate governance policies of owners/operators. Entities under the TSA security directives call for information to be provided to the TSA as required under the Cybersecurity Implementation Plan. A firm told the Chamber that it has "a cybersecurity awareness program that requires all who have system access (e.g., contractors, employees, and interns) to undertake training within 30 days of onboarding and every 2 years thereafter."

§ 101.650 Paragraph (e): Risk Management

This section would establish three levels of Cybersecurity Assessment and risk management: (1) conducting annual Cybersecurity Assessments; (2) completing penetration testing upon renewal of a VSP, FSP, or OCS FSP; and (3) ensuring ongoing routine system maintenance. The CySO would ensure that these activities, which are listed in Sections 11 and 12 of the Cybersecurity Plan, are documented and completed.[24]

- Section III.G.b–c of the TSA security directive already requires a biannual cybersecurity vulnerability assessment. Also, section III.E.1 of the directive already requires a patch management strategy to ensure that critical security updates on Critical Cyber Systems are up to date.[25]

§ 101.650 Paragraph (f): Supply Chain

This section would specify measures to manage cybersecurity risks in the supply chain of covered entities comparable to the "Identify" function of NIST's Cybersecurity Framework (CSF).[26]

---

[22] https://www.federalregister.gov/d/2024-03075/p-273

[23] TSA security directive, p. 5.

[24] https://www.federalregister.gov/d/2024-03075/p-279

[25] TSA security directive, pp. 7, 9.

[26] https://www.federalregister.gov/d/2024-03075/p-292

- Supply chain security requirements are often determined by corporate policies and the terms and conditions established with communication and technology vendors.

§ 101.650 Paragraph (g): Resilience

This section would ensure that covered entities can recover from major cyber incidents with minimal impact on critical operations. The proposed rule would require the owner/operator or the CySO to ensure that the following response and recovery activities, such as reporting any cyber incidents to the Coast Guard, developing and implementing a Cyber Incident Response Plan, and periodically validating its effectiveness.

- Disaster recovery/resilience (e.g., backing up data) requirements are already specified in the owner/operator's Cybersecurity Incident Response Plan for the Critical Cyber Systems under section III.F of the TSA security directive.[27]

§ 101.650 Paragraph (h): Network Segmentation

This section would require the CySO to ensure that a covered network is segmented and document those activities in a Cybersecurity Plan. Network integrity is a key provision under the "Protect" function of the NIST CSF. The Coast Guard says that network architectures vary widely based on the operations of a vessel or facility. Separating IT and OT networks is challenging, and it becomes increasingly difficult with an increase in the various devices connected to the network. Nonetheless, the Coast Guard recognizes that the IT and OT interface represents a weak link.[28]

- Network segmentation is already required under section III.B of the TSA security directive.[29]

§ 101.650 Paragraph (i): Physical Security

This section would specify that owners/operators and CySOs would manage physical access to IT and OT systems. As described in the "Protect" function of the NIST CSF, physical security protects critical IT and OT systems by limiting access to the human-machine interface (HMI). The Coast Guard notes that the proposed physical security measures would supplement the existing VSA, facility security assessments (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, the CySO would designate areas restricted to authorized personnel and secure HMIs and other hardware. The CySO would also establish policies to restrict the use of unauthorized media and hardware. These proposed provisions would mirror existing Coast Guard policy outlined in NVIC 01–20.[30]

---

[27] TSA security directive, pp. 8–9.

[28] https://www.federalregister.gov/d/2024-03075/p-303

[29] TSA security directive, p. 5.

[30] https://www.federalregister.gov/d/2024-03075/p-306

- The management of physical access to IT and OT systems are already managed under Maritime Security and Transportation Worker Identification Credential regulations. The same levels of restriction apply to all on-site personnel.[31]

II. REQUIREMENTS OF THE NPRM (SELECTED POINTS)

§ 101.605—Applicability (*FR*, pp. 13408, 13508)

The proposed rule would expand the Coast Guard's regulations related to cybersecurity by establishing minimum cybersecurity requirements for the marine transportation system within the MTSA regulations. Similar to the existing requirements in 33 CFR parts 104, 105, and 106, the Coast Guard says that it would give owners/operators the flexibility to determine the best way to implement and comply with these new requirements, applicable to the owners/operators of covered vessels, facilities, and OCS facilities.

- **Consider establishing a separate rulemaking for vessels.** Some in industry believe that the Coast Guard should consider establishing a separate rulemaking addressing vessels' unique circumstances and needs. The NPRM, however, seems to treat all the covered entities equally.

    - It is common knowledge that vessels operate in distinct environments and are frequently away from shore. OT vendors that serve the marine industry function at differing levels of cybersecurity maturity compared to those serving other covered entities. One company told the Chamber that "OT found on a vessel is very different. In many cases, we are unable to access the OT because it is controlled by the vendors, some of which are foreign owned. The Coast Guard's rulemaking should align with international cybersecurity standards."

    - Vessels' OT cybersecurity practices differ from other types of critical infrastructure, including how ships are designed and built. Vessels, which can be 10 to 20 years of age, often employ cybersecurity controls that are unique to them. In OT environments, for example, vessel cybersecurity is maintained through network security management, perimeter security, and rigorous segmentation, among other safeguards not accounted for in the NPRM.

    - Some industry groups are proposing vendor accountability for OT-specific requirements in the Coast Guard's proposal. The Coast Guard should partner with vendors and CISA to bolster the cybersecurity of vessels. A company told the Chamber, "We are unable to push practical, business-to-business requirements

[31] 33 CFR § 104.200—Owner/operator. 33 CFR 104.200(b)(12)(iii).
https://www.law.cornell.edu/cfr/text/33/104.200

33 CFR § 104.270—Security measures for restricted areas. 33 CFR 104.270(c)(6).
https://www.law.cornell.edu/cfr/text/33/104.270

33 CFR § 105.260—Security measures for restricted areas. 33 CFR 105.260(c)(6).
https://www.law.cornell.edu/cfr/text/33/105.260

because we typically lack access to vendor-controlled OT, and the proposed regulation does not reflect this reality."

- **Coordinate with the Department of the Interior's Bureau of Safety and Environmental Enforcement (BSEE) regarding OCS facilities.** Owing to the shared authority on the OCS by the Coast Guard and BSEE, as called for under the Outer Continental Shelf Lands Act (OCSLA), industry groups urge the Coast Guard to exempt offshore facilities from 33 CFR 106.

    - Instead, the Coast Guard and BSEE should leverage their 2012 memorandum of understanding (MOU) on promoting interagency consistency in the regulation of OCS facilities to develop a memorandum of agreement (MOA) that is specific to cybersecurity. An MOA developed under the terms of the overarching MOU would better define the agencies' respective roles and shared responsibilities vis-à-vis various OCS facilities. Examples include developing compatible policies and regulations, fostering communication and cooperation between the agencies and the business community, and optimizing stakeholders' expertise and resources. The Coast Guard and BSEE have a number of MOAs in place but not one that is specific to cybersecurity.

    - Buttressing this thinking is a recommendation made by the Government Accountability Office (GAO) in a 2022 report on the offshore oil and gas sector. The GAO urged BSEE to "immediately develop and implement a strategy to address offshore infrastructure risks. Such a strategy should include an assessment and mitigation of risks, and identify objectives, roles, responsibilities, resources, and performance measures, among other things."

    - The most effective way to ensure a robust cybersecurity posture on the OCS is to involve primary OCS regulators so that a harmonized and holistic approach to governance can be taken. Industry groups do not believe this can be done under the proposed rule because it would only apply to the 33 OCS facilities currently subjected to 33 CFR 106 requirements and would not address drilling units because they are all foreign-flagged vessels. There are over 1,600 OCS facilities in the Gulf of Mexico and over 400 of these are staffed (e.g., they have personnel on them 24/7). There are 23 fixed platforms on the California OCS, with 22 of these entities being staffed. None of the California platforms meet the MTSA applicability threshold in 33 CFR 106.

    - Further, OCS operations (e.g., drilling and production) fall under BSEE authorities, and most IT or OT systems on OCS facilities perform functions related to operations that come under BSEE's jurisdiction, not the Coast Guard's.

    - Attempting to implement cybersecurity regulations on the OCS via the limited scope of the MTSA would result in an incomplete effort and create the possibility that OCS operators may eventually have to contend with overlapping and/or conflicting regulations from BSEE and the Coast Guard.

The Coast Guard should enable a more risk-based approach to managing cybersecurity. Overall, covered entities should be empowered to conduct penetration testing, deploy software updates (patching), determine the frequency of drills and exercises, and train personnel in partnership with the government but based on a company's standard operating procedures.

§ 101.615—Definitions (*FR*, pp. 13409, 13508)

The Coast Guard proposes to include terms and definitions for *Cyber incident, Cyber risk, Cyber threat,* and *Cybersecurity vulnerability. Cyber incident* would relate to *Information Systems* and would be inclusive of both *Information Technology* and *Operational Technology,* all of which the Coast Guard is proposing to define. In addition, the Coast Guard proposes newly defined terms that are applicable to maritime cybersecurity, including *Critical Information Technology or Operational Technology systems, Cyber Incident Response Plan, Cybersecurity Officer* or *CySO,* and *Cybersecurity Plan.*

The NPRM indicates that the Coast Guard consulted several authoritative sources for the new terms and definitions, including defense legislation, CISA resources, and NIST's Computer Security Resource Center (CSRC) Glossary. The CSRC glossary includes terminology from the final versions of NIST's cybersecurity and privacy publications. The Chamber believes that consistency among the Coast Guard's MTSA program and the multiple other federal data security, cybersecurity, and reporting requirements are important. The Coast Guard's proposed rule puts forward definitions related to cybersecurity that generally seem to track closely with NIST definitions.

The Chamber believes that the Coast Guard (as we would with any similarly situated agency) should not depart from NIST definitions unless they need to be tailored to maritime operations (see the Appendix).

§ 101.620—Owner/Operator (*FR*, p. 13410, 13510)

This proposed section would require each owner/operator of a covered entity to assign qualified personnel to develop a Cybersecurity Plan and ensure that the plan incorporates detailed preparation, prevention, and response activities for cybersecurity threats and vulnerabilities.

> (b) For each vessel, facility, or OCS facility, the owner or operator must—
>
> (1) Ensure a Cybersecurity Plan is developed, approved, and maintained;
>
> (2) Define in Section 1 of the Cybersecurity Plan the cybersecurity organizational structure and identify each **person** [bolding added] exercising cybersecurity duties and responsibilities within that structure, with the support needed to fulfill those obligations;[32]

[32] https://www.federalregister.gov/d/2024-03075/p-801

- In subsection (b)(2), it is unclear to the Chamber whether a "person" is synonymous with "role"?

§ 101.625—Cybersecurity Officer (*FR*, pp. 13410, 13510)

According to the NPRM, the CySO may be a full-time, collateral, or contracted position. The same person may serve as the CySO for more than one vessel, facility, or OCS facility. The CySO would need to have general knowledge of a range of issues relating to cybersecurity, such as cybersecurity administration, relevant laws and regulations, current threats and trends, risk assessments, inspections, control procedures, and procedures for conducting exercises and drills. When considering assigning the CySO role to the existing security officer, the owner/operator should consider the depth and scope of these new responsibilities in addition to existing security duties.[33]

The Coast Guard's proposal states, "The CySO would have the authority to assign cybersecurity duties to other personnel; however, the CySO would remain responsible for the performance of these duties." Still, industry believes that more than one person is needed for the CySO role due to the breadth of responsibilities outlined in the rulemaking—conducting penetration testing, handling threat intelligence, managing vulnerabilities, monitoring IT and OT systems, preparing the Cybersecurity Plan, responding to incidents, training on cybersecurity, and understanding technical standards, and more.

Excerpt From the Coast Guard's NPRM

The most important duties [the] CySO would perform include ensuring development, implementation, and finalization of a Cybersecurity Plan; auditing and updating the Plan; ensuring adequate training of personnel; and ensuring the U.S.-flagged vessel, facility, or OCS facility is operating in accordance with the Plan and in continuous compliance with this subpart. **The CySO would have the authority to assign cybersecurity duties to other personnel; however, the CySO would remain responsible for the performance of these duties** [bolding added].[34]

- The Chamber believes that the Coast Guard should allow the CySO to feature a group of people that perform cybersecurity duties similar to the approach taken by the *Navigation and Vessel Inspection Circular (NVIC) 01-20* and the TSA security directive, rather than overly burden a single person.

[33] https://www.federalregister.gov/d/2024-03075/p-226

[34] https://www.federalregister.gov/d/2024-03075/p-227

Excerpt From the Maritime Cybersecurity Assessment and Annex Guide (MCAAG)[35]

Identify a Cybersecurity Officer (CySO)
The FSO [Facility Safety Officer] should identify a person or group of people who can speak authoritatively about the cyber[-]enabled systems, networks[,] and cybersecurity protections in the facility, and who can partner with the FSO to create the Cyber Annex. The CySO may be a single person from the information technology or cybersecurity organization of the facility, **or it may be a group of people** [bolding added]. There is nothing precluding the FSO and the CySO from being the same person, provided they have adequate cybersecurity training and knowledge.

- As proposed by the Coast Guard, the CySO's duties would go well beyond cybersecurity to include managing physical security controls for IT and OT systems.[36] Since the CySO focuses on IT and OT and cybersecurity systems and equipment, with associated maintenance, this thinking should be reconsidered. Physical security should be addressed separately. There is lack of consistency across governing agencies on this issue.

- The requirements listed in § 101.625(d)(8)–(9), which both emphasize training, seem redundant and could perhaps be merged.

(8) Ensure the cybersecurity awareness and vigilance of personnel through briefings, drills, exercises, and training;

(9) Ensure adequate cybersecurity training of personnel;[37]

- It is not clear to the Chamber how the list of 12 characteristics establishes whether a person is qualified to perform as the CySo.[38] "The knowledge, skills, or training required to be the CySO are daunting—it's not clear who would qualify," a business told the Chamber.

§ 101.635—Drills and Exercises (*FR*, pp. 13411, 13511)

Under this proposed section, cybersecurity drills and exercises would be required to test the proficiency of vessel, facility, and OCS facility personnel in assigned cybersecurity duties and in the effective implementation of the VSP, FSP, OCS FSP, and Cybersecurity Plan. Also,

[35] MCAAG, January 2023, p. 1.
https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment%20%20Annex%20Guide%20(MCAAG)_released%2023JAN2023.pdf

[36] https://www.federalregister.gov/d/2024-03075/p-237
https://www.federalregister.gov/d/2024-03075/p-849

[37] https://www.federalregister.gov/d/2024-03075/p-818
https://www.federalregister.gov/d/2024-03075/p-819

[38] https://www.federalregister.gov/d/2024-03075/p-826

drills and exercises should assist the CySO in identifying any related cybersecurity deficiencies that need to be addressed.

- The Chamber contends that drills and exercises should be clarified and scaled based on a covered entity's assessment of its cybersecurity risk.

- A firm told the Chamber, "The frequency of drills and exercises should be based on risks to a facility, and the tempo and scale of drills versus exercises should be modified accordingly."

- The proposed frequency of drills occurring every three months is not reasonable—especially because of the resources that drills would demand of covered entities—and should occur commensurate with risk.

> (b) *Drills*. (1) The CySO must ensure that at least one cybersecurity drill is conducted every 3 months. Cybersecurity drills may be held in conjunction with other security or non-security drills, where appropriate. . . .[39]
>
> (c) *Exercises.* (1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.[40]

- Drills come across as a paper exercise that could result in a misallocation of company resources. The exercises may be more valuable to private entities than drills.

- If the Coast Guard is unable to accommodate a drill and exercise schedule that is risk based, industry proposes that the cybersecurity should be folded into covered entities' existing drill and exercise schedules.

§ 101.640 Records and Documentation (*FR*, pp. 13411, 13512)

This section would require owners/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 two years and be made available to the Coast Guard upon request. The records can be kept in paper or electronic format and must be protected against unauthorized access, deletion, destruction, amendment, and disclosure. Records that each vessel, facility, or OCS facility keep would vary because each organization would maintain records specific to its operations.

At a minimum, the records would have to capture the following activities: training, drills, exercises, cybersecurity threats, incidents, and audits of the Cybersecurity Plan as set forth in the

[39] https://www.federalregister.gov/d/2024-03075/p-881

[40] https://www.federalregister.gov/d/2024-03075/p-884

cited recordkeeping requirements above and made applicable to records under this subpart per § 101.640.[41]

- A number of industry groups contend that the two-year recordkeeping mandate could be quite costly compared to its value proposition.

§ 101.650—Cybersecurity Measures (*FR*, pp. 13411, 13512)

First, at a relatively high level, the Chamber is interested in better understanding what the Coast Guard was not getting from covered entities' use of the Cyber Annex—which supports a facility security plan, or FSP—under the 2023 the *Maritime Cybersecurity Assessment and Annex Guide* (MCAAG). The MCAAG was developed in partnership with a number of maritime stakeholders, such as the Coast Guard, the National Maritime Security Advisory Committee, and Area Maritime Security committees.

- The MCAAG and Cyber Annex provide facilities with a framework to implement MTSA regulations in pursuit of addressing vulnerabilities and related to computer networks and information systems.[42]

- Facility owners/operators are afforded flexibility in adhering to specific guidance or tools that best meet their needs as long as the regulatory requirements are met.

- Industry groups tell the Chamber that they appreciate the Coast Guard's Cyber Annex Template, which helps them make connections between the physical security vulnerabilities identified in an FSA and the cybersecurity protections recommended in the Cyber Annex.

- A company said that "much thought, time, and resources have gone into creating our Cyber Annex." Industry, the company added, "should not shift entirely away from the Cyber Annex," which the proposed rule suggests.

- An alternative approach to the rulemaking, which entails having the Coast Guard mandate security measures, could be a revamped annex process. This approach could enable the owner/operator to describe its Cybersecurity Plan and Annex, including having the Coast Guard ask more detailed and probing questions during inspections to help entities identify gaps in their cybersecurity programs under MTSA.

    - For example, with regard to the **cybersecurity training requirements**, the Coast Guard could ask how the company fosters a culture of cybersecurity awareness.

---

[41] https://www.federalregister.gov/d/2024-03075/p-258

[42] https://www.federalregister.gov/d/2024-03075/p-141

https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Maritime%20Cyber%20Assessment%20%20Annex%20Guide%20(MCAAG)_released%2023JAN2023.pdf

Officials could ask how the owner/operator differentiates training according to roles and responsibilities vis-à-vis the Cybersecurity Plan?[43]

- With respect to **drills and exercises**, the Coast Guard could ask how an entity conducts drills and exercises to test its capabilities and resilience and how it communicate lessons learned to key personnel.[44] The Coast Guard could consider providing owners/operators scenarios for conducting such drills (e.g., ways in which to test emergency response capabilities).

- The Coast Guard could ask about an organization's **supply-chain security measures** as opposed to mandating specific requirements.[45]

- A firm told the Chamber, "We need to move beyond the assumption that while some activities prescribed by regulation is good, more and more activities are better. To the contrary, adding relative busy work, such as the quarterly drills beyond those already required under MTSA, is not necessarily constructive. Box-checking rules, while not the Coast Guard's intention, would divert resources from initiatives targeted to enhancing our resilience. The Coast Guard and industry could benefit from reflecting on TSA's experience with the first iteration of the TSA security directive."

- TSA's initial security directive was calibrated to apply to the largest owners/operators and then only to the critical pipeline assets operated by a company. The Coast Guard's proposed rule would apply significant cybersecurity requirements to all covered entities regardless of their risk posture, sophistication, size, and so forth. "Should a dock that handles wood chips or gypsum be held to the same standards as a refinery? Shouldn't the requirements be adjusted according to risk?" a business asked the Chamber.

  "Along these same lines," the business added, "the Coast Guard's mission is to ensure that U.S. waterways remain navigable. If a facility's cyber systems are fully segregated from dock operations and would not be relevant in a TSI [transportation security incident], why should that company need to comply with the costly maritime cybersecurity regulations?"

- Another unintended consequence of requirements is the demotivating impact that they would likely have on cybersecurity and IT professionals—many of whom are dedicated to cybersecurity but have not signed on for a role that is heavy on regulatory compliance. Given the cybersecurity skills shortage that is widely acknowledged, businesses cannot afford to have attrition in their cybersecurity and IT departments.

---

[43] https://www.federalregister.gov/d/2024-03075/p-275
https://www.federalregister.gov/d/2024-03075/p-913

[44] *FR*, pp. 13411, 13511.

[45] https://www.federalregister.gov/d/2024-03075/p-939

Second, this section of the Chamber's letter captures specific cybersecurity measures (note the text in dark green) that the Coast Guard spotlights to identify risks, detect threats and vulnerabilities, protect critical systems, and recover from cyber incidents. The proposed rule notes that any intentional gaps in cybersecurity measures would be documented as accepted risks under proposed § 101.630(c)(12). Further, if owners/operators are unable to comply with the requirements of this subpart, they may seek a waiver or an equivalence determination under proposed § 101.665.[46]

(a) Account security measures. Each owner/operator of a vessel, facility, or OCS facility must ensure, at a minimum, the following account security measures are in place and documented in section 7 of the Cybersecurity Plan.[47]

The NPRM says that this provision would identify minimum account security measures to protect critical IT and OT systems from unauthorized cyber access and limit the risk of a cyber incident. Access control is a foundational category and is highlighted as a "Protect" function of NIST's CSF.

- The proposal would require owners/operators to lock out individuals after repeated failed login attempts on IT and OT systems.[48]
    - However, forced lockouts can be a dangerous configuration to apply to an OT system.
    - If legitimate personnel are unable to access and control a process control system in an emergency, this could lead to escalating consequences.
    - Industry suggests that the lockout requirement should be reconsidered in the context of multi-factor authentication, or MFA. It should be narrowed to apply to secure remote access.

(b) Device security measures. Each owner/operator or designated CySO of a vessel, facility, or OCS facility must ensure the following device security measures are in place and documented in section 6 of the Cybersecurity Plan.[49]

§ 101.650(b)(1) of the proposed rule would require owners/operators of covered entities to develop and maintain a list of company-approved hardware, firmware, and software that may be installed on IT or OT systems. This approved list would be documented in the Cybersecurity Plan.[50]

---

[46] https://www.federalregister.gov/d/2024-03075/p-260

[47] https://www.federalregister.gov/d/2024-03075/p-897

[48] https://www.federalregister.gov/d/2024-03075/p-898

[49] https://www.federalregister.gov/d/2024-03075/p-905

[50] https://www.federalregister.gov/d/2024-03075/p-506

(b)(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.[51]

- The whitelisting (aka allowlisting) requirement should be removed for both IT and OT.
    - The cost of maintaining a list of approved hardware, firmware, and software in the context of IT systems is a case where the cost of the specific control dwarves the benefit of the measure. For OT, it's questionable if the firmware whitelist actually drives value. There is no way to prevent non-whitelisted firmware from being installed.
    - The requirement for whitelisting presents a significant issue for IT systems due to the quantity (e.g., thousands) of applications that a covered entity could be expected to manage.
    - Issues with OT pertain specifically to vendor control of some OT systems. Whitelisting would require support from, testing, and approval from these vendors. This would affect the ability to control compliance for some sites as vendors may be the only entities with such access.
    - A company told the Chamber that "this is likely a legacy error based on this part's derivation from parts 104 and 105 in which owners/operators have the ability to control physical security."
- Some in industry question the feasibility of ensuring that **applications running executable code** must be disabled by default on critical IT and OT systems.

(b)(2) Ensure **applications running executable code** [bolding added] must be disabled by default on critical IT and OT systems. Exemptions must be justified and documented in the Cybersecurity Plan.[52]

(c) Data security measures. Each owner/operator or designated CySO of a vessel, facility, or OCS facility must ensure that the following data security measures are in place and documented in section 4 of the Cybersecurity Plan.[53]

Subsection (c)(2) says that all data must be encrypted, but this proposed requirement is not supported by all technology used in the OT space.

[51] https://www.federalregister.gov/d/2024-03075/p-906

[52] https://www.federalregister.gov/d/2024-03075/p-907

[53] https://www.federalregister.gov/d/2024-03075/p-910

(c)(2) All data, both in transit and at rest, must be encrypted using a suitably strong algorithm.[54]

(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.[55]

Under this portion of the Coast Guard's proposal, certain cybersecurity training requirements are required of owners/operators. The Coast Guard notes that security training is a key aspect of the MTSA. Relevant provisions in 33 CFR already require personnel to have knowledge, through training or equivalent job experience, in the "Recognition and detection of dangerous . . . devices." Since 2020, the Coast Guard has interpreted this requirement to include relevant cybersecurity training.[56]

The proposed rulemaking says that while formal training may be appropriate, the Coast Guard would not mandate a format of training. However, the training would have to minimally cover relevant provisions of an organization's Cybersecurity Plan (e.g., detecting cybersecurity threats and reporting cyber incidents to the CySO).

- The Chamber thinks that subsection (d)(1)(i) is vague to some businesses. It is unclear whether covered entities' cybersecurity personnel and the Coast Guard would agree on what constitutes the "relevant provisions" of a Cybersecurity Plan.

- There is concern, too, about subsection (d)(1)(iii), which calls for "All personnel with access to the IT or OT systems, including contractors" to be trained in techniques used to "circumvent cybersecurity measures." A firm told the Chamber that "this blanket approach to training is perhaps suboptimal. Teaching 'all personnel' to bypass security measures strikes us as a bad idea."

(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 [on] the following topics:
(i) **Relevant provisions** [bolding added] of the Cybersecurity Plan;
(ii) Recognition and detection of cybersecurity threats and all types of cyber incidents;[57]
(iii) Techniques used to **circumvent cybersecurity measures** [bolding added];

[54] https://www.federalregister.gov/d/2024-03075/p-912

[55] https://www.federalregister.gov/d/2024-03075/p-913

[56] https://www.federalregister.gov/d/2024-03075/p-275

[57] *FR*, p. 13512.

- Subsection (d)(2)(ii) calls for key personnel to keep current on the threat landscape and defensive measures. Some covered entities believe that this requirement may be challenging relative to available resources and so forth.

(ii) Maintaining current knowledge of changing cybersecurity threats and countermeasures.[58]

- The Chamber urges the Coast Guard to shift the effective date of this rulemaking related to training and "gaining system access" to 30 days from 5 days. While we understand the Coast Guard's desired time frame, 5 days is largely impractical, even for well-resourced entities. Our recommended change is redlined in the table below.

(d)(3) All personnel must complete the training specified in paragraphs (d)(1)(ii) through (v) of this section by [DATE 180 DAYS AFTER EFFECTIVE DATE OF THE FINAL RULE], and annually thereafter. Key personnel must complete the training specified in paragraph (d)(2) of this section by [DATE 180 DAYS AFTER EFFECTIVE DATE OF THE FINAL RULE], and annually thereafter, or more frequently as needed. Training for new personnel not in place at the time of the effective date of this rule must be completed within ~~5~~ 30 days of gaining system access, but no later than within 30 days of hiring, and annually thereafter. Training for personnel on new IT or OT systems not in place at the time of the effective date of this rule must be completed within 5 days of system access, and annually thereafter. All personnel must complete the training specified in paragraph (d)(1)(i) within 60 days of receiving approval of the Cybersecurity Plan. The training must be documented and maintained in the owner's or operator's records in accordance with 33 CFR 104.235 for vessels, 105.225 for facilities, and 106.230 for OCS facilities.[59]

(e) Risk management. Each owner/operator or designated CySO of a vessel, facility, or OCS facility must ensure that the following measures for risk management are in place and documented in sections 11 and 12 of the Cybersecurity Plan.[60]

This part of the rulemaking would establish three levels of Cybersecurity Assessment and risk management: (1) conducting annual Cybersecurity Assessments; (2) completing penetration testing upon renewal of a VSP, FSP, or OCS FSP; and (3) ensuring ongoing routine system maintenance. The Coast Guard says that the CySO needs to ensure that these activities are documented and completed in the Cybersecurity Plan.[61]

The NPRM says that while Cybersecurity Assessments provide a valuable picture of potential security weaknesses, penetration testing could add additional context by demonstrating whether malicious actors can leverage such weaknesses. Penetration tests (aka pen testing) can help prioritize resources based on what poses the most risk.[62]

---

[58] https://www.federalregister.gov/d/2024-03075/p-922

[59] https://www.federalregister.gov/d/2024-03075/p-923

[60] https://www.federalregister.gov/d/2024-03075/p-924

[61] https://www.federalregister.gov/d/2024-03075/p-279

[62] https://www.federalregister.gov/d/2024-03075/p-283

(2) *Penetration Testing.* In conjunction with FSP, OCS FSP, or VSP renewal, the owner or operator or designated CySO must ensure that a penetration test has been completed. Following the penetration test, all identified vulnerabilities must be included in the FSA or VSA, in accordance with 33 CFR 104.305, 105.305, and 106.305.[63]

- Penetration tests are generally challenging for OT because entire sites must be shut down to perform it. The minimum or maximum duration of a penetration test depends greatly on the size of an off-shore facility, ship, or terminal and the scope of testing. Pen tests are currently prioritized based on the criticality of an asset. A company told the Chamber, "Typically, pen testing can easily last a week—and it may last two weeks for a larger facility."

- It is unclear what the Coast Guard's expectation is for a pen test.

- Industry is interested whether the Coast Guard would accept pen testing of—

    - The same architecture but simulated in a lab or virtual environment.
    - Only noncritical systems in the IT environment.

- Additional concerns regarding penetration tests relate to shipping. A private entity told the Chamber that "active vessels don't stop for very long when docked. The loading or unloading of cargo can span anywhere between 24 hours to two to three days. This would not be a good time to conduct a pen test." The private entity added that "it is worth noting that pen testing of OT systems requires the support, and possibly the physical presence, of specialized OT vendor representatives. Given the many OT systems onboard a ship provided by discrete vendors, pen testing is a significant logistical burden on the industry."

- Routine system maintenance requires an ongoing effort to identify vulnerabilities and would include scanning and reviewing known exploited vulnerabilities (KEVs) by documenting, tracking, and monitoring them. These proposed provisions would mirror the security system and equipment maintenance requirements in 33 CFR 104.260 for vessels, 33 CFR 105.250 for facilities, and 33 CFR 106.255 for OCS facilities.

(e)(3) Routine system maintenance. Each owner or operator or a designated CySO of a vessel, facility, or OCS facility must ensure [that] 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** [bolding added];[64]

---

[63] https://www.federalregister.gov/d/2024-03075/p-931

[64] https://www.federalregister.gov/d/2024-03075/p-933

- While the Chamber understands the Coast Guard's sense of urgency regarding patching, it may be inappropriate to use "without delay" in the cyber context. A business told the Chamber that "critical maintenance, including major software updates, are best done during a ship's periodic special survey where vendor support is onboard. If patching is done 'without delay,' this likely means while the ship is in service and sailing between ports. (Similarly, it is not advisable to make changes to a ship while transferring cargo in port.) Patching, while a ship is in service, can disable it, leaving it vulnerable to a loss of navigation. The risk of 'bricking' a ship system during a software update is a real possibility."

  Thus, the NPRM's call to ensure that the patching or the implementation of documented compensating controls for all KEVs in critical IT or OT systems "without delay," should be given further consideration by the Coast Guard and industry.

- It would be helpful for the Coast Guard to clarify what it means by "connected to" in subsection (e)(3)(v).

> (e)(3)(v) Ensure no OT is **connected to** [bolding added] the publicly accessible internet unless explicitly required for operation, and verify that, for any remotely accessible OT system, there is a documented justification; and[65]

(f) Supply chain. Each owner/operator or designated CySO of a vessel, facility, or OCS facility must ensure that the following supply-chain measures are in place and documented in section 4 of the Cybersecurity Plan.[66]

A provision in the supply chain section stipulates that owners/operators must establish a process through which all IT and OT vendors or service providers rapidly notify them or the CySO of any cybersecurity vulnerabilities, incidents, or breaches.

> (f)(2) Establish a process through which all IT and OT vendors or service providers notify the owner or operator or designated CySO of any cybersecurity vulnerabilities, incidents, or breaches, without delay;

- The Coast Guard appears to be mandating that covered entities establish a broad reporting program for their suppliers and vendors. Such an undertaking could be considerable to develop, manage, and resource. Among other considerations, the Chamber believes that a workable notification threshold—such as one based on the materiality or the significance of a vulnerability, an incident, or a breach—should be developed in partnership with the business stakeholders for subsection (f)(2).

[65] https://www.federalregister.gov/d/2024-03075/p-937

[66] https://www.federalregister.gov/d/2024-03075/p-939

III. REPORTABLE CYBER INCIDENT

The Chamber appreciates the Coast Guard's request for covered entities' views on reportable cyber incidents. At the time of this writing, the Chamber is preparing a comment letter to CISA in response to the agency's proposed rule on CIRCIA reporting requirements, with comments being due on July 3, 2024. We will provide a copy of the letter to the Coast Guard once it is submitted. In the interim, three points are worth emphasizing:

First, among other things, the Coast Guard is soliciting comments on an optimal approach for reporting cyber incidents. The Chamber strongly believes that a report of a *covered cyber incident* by a covered entity to CISA under the CIRCIA program or to the Coast Guard under this NPRM should satisfy the reporting requirements of both agencies.

Second, the Coast Guard is on the correct path when it notes that this approach "could allow more efficient use of DHS' cybersecurity resources and may advance the cybersecurity vision laid out by Congress in [CIRCIA], which will be implemented by regulations that are still under development. Information submitted to CISA would be shared with the Coast Guard, ensuring continued efficient responses." Further, the Coast Guard seems to suggest that if followed this approach, "to the extent that the reporting obligation imposed by this NPRM constitutes a requirement to report 'substantially similar information . . . within a substantially similar timeframe' when compared to a rule implementing CIRCIA, covered entities may be excused from any duplicative reporting obligations under the CIRCIA rulemaking."[67]

It is encouraging to see that the Coast Guard is trying to adopt some of the key recommendations outlined in DHS' September 2023 report on streamlining the reporting of cyber incidents to better protect the nation's critical infrastructure.[68]

Third, while the *substantially similar reporting exception* (aka a CIRCIA agreement or an interagency agreement) may not become effective until the CIRCIA rule is final, the Chamber urges the Coast Guard to work with CISA and TSA to explore opportunities to reduce duplicative reporting of covered cyber incidents impacting private entities likely covered under CIRCIA and the Coast Guard's NPRM.

Excerpt From CISA's Proposed Rule on CIRCIA

CISA intends to work with other Federal departments and agencies to explore opportunities to reduce duplicative reporting of covered cyber incidents through a proposed **substantially similar reporting exception** [bolding added] to CIRCIA. Under this exception, which is authorized under 6 U.S.C. 681b(a)(5)(B), a covered entity that is required by law, regulation, or contract to report information to another Federal entity that is substantially similar to the information that must be reported under CIRCIA and is required to submit the report in a substantially similar timeframe to CIRCIA's reporting

[67] *FR*, pp. 13409–13410.

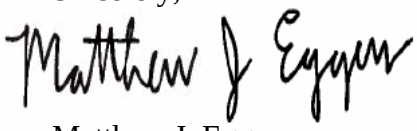
[68] DHS, "DHS Issues Recommendations to Harmonize Cyber Incident Reporting for Critical Infrastructure Entities," September 19, 2023. https://www.dhs.gov/news/2023/09/19/dhs-issues-recommendations-harmonize-cyber-incident-reporting-critical

deadlines, may be excepted from reporting it again under CIRCIA. Per the statute, **for covered entities to be able to leverage this specific exception, CISA and the respective Federal entity must enter into an interagency agreement, referred to as a CIRCIA Agreement** [bolding added], and establish an information sharing mechanism to share reports. To the extent practicable, CISA is committed to working in good faith with its Federal partners to have CIRCIA Agreements finalized before the effective date of the final rule.[69]

***

Thank you for the opportunity to provide the Coast Guard comments on the NPRM on Cybersecurity in the Marine Transportation System. If you have any questions or need more information, please do not hesitate to contact me (meggers@uschamber.com).

Sincerely,



Matthew J. Eggers
Vice President
Cyber, Space, and National Security
Policy Division
U.S. Chamber of Commerce

[69] *FR*, p. 23654.

APPENDIX

The Appendix features the Coast Guard's proposed terms and definitions to be included in the proposed rule and the comparable NIST terms and definitions, where available, in blue text.[70] In the main, the Coast Guard's proposed terms and definitions appear similar to NIST's, which the Chamber supports.

- *Approved list* means an owner['s] or operator's authoritative catalog for products that meet cybersecurity requirements.

- Approved list. No comparable NIST definition.

- *Backup* means a copy of physical or virtual files or databases in a secondary location for preservation. It may also refer to the process of creating a copy.

- Backup. A copy of files and programs made to facilitate recovery if necessary.

- *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.

- Capability, **Credentials** [bolding added here and elsewhere in the Appendix] and Authentication Management. An ISCM [information security continuous monitoring] capability that ensures that people have the credentials and authentication methods necessary (and only those necessary) to perform their duties, while limiting access to that which is necessary.

- *Critical Information Technology (IT) or **Operational Technology (OT)** systems* means any Information Technology or Operational Technology system used by the vessel, facility, or OCS facility that, if compromised or exploited, could result in a transportation security incident, as determined by the Cybersecurity Officer (CySO) in the Cybersecurity Plan. Critical IT or OT systems include those business support services that, if compromised or exploited, could result in a transportation security incident. This term includes systems whose ownership, operation, maintenance, or control is delegated wholly or in part to any other party.

- **Operational technology.** Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

[70] The terms and definitions in blue text are taken from the CSRC Glossary. https://csrc.nist.gov/glossary

- *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. Actions taken through the use of an information system or network that result in an actual or **potentially** adverse effect on an information system, network, and/or the information residing therein. See incident. See also event, security-relevant event, and intrusion.

Note that the Chamber believes that policy should link reporting to confirmed—not potential—cyber incidents. Businesses need clarity in reporting requirements, which should be targeted to well-defined and verified cyber incidents. Comparatively loose definitions would yield extraneous information that does not improve the situational awareness of the government and other critical infrastructure organizations.[71]

- *Cyber Incident Response Plan* means a set of predetermined and documented procedures to respond to a cyber incident. It is a document that gives the owner or operator or a designated Cybersecurity Officer (CySO) instructions on how to respond to a cyber incident and pre-identifies key roles, responsibilities, and decision makers.

- Cyber Incident Response Plan. No comparable NIST definition.

- *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.

- Cyber threat. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability.

- *Cybersecurity Assessment* means the appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations,

---

[71] See the U.S. Chamber's February 2, 2024, letter to the Defense Department (DoD), the General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA) regarding their proposal to amend the Federal Acquisition Regulation (FAR) on Cyber Threat and Incident Reporting and Information Sharing. Note, too, pp. 15–22 of the Chamber's letter on *security incident* reporting harmonization. https://www.regulations.gov/comment/FAR-2021-0017-0062

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.

- Assessment. The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

- *Cybersecurity Officer*, or CySO, means the person(s) designated as responsible for the development, implementation, and maintenance of the cybersecurity portions of the Vessel Security Plan (VSP), Facility Security Plan (FSP), or Outer Continental Shelf (OCS) FSP, and for liaison with the Captain of the Port (COTP) and Company, Vessel, and Facility Security Officers.

- Chief information officer. No comparable NIST definition.

- *Cybersecurity Plan* means a plan developed to ensure [the] application and implementation of cybersecurity measures designed to protect the owner's/operator's systems and equipment, as required by this part. A Cybersecurity Plan is either included in a VSP, FSP, or OCS FSP, or is an annex to a VSP, FSP, or OCS FSP.

- Cybersecurity Plan. No comparable NIST definition.

- *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 risk. An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts [on] organizational operations (i.e., mission, functions, image, reputation) and assets, individuals, other organizations, and the Nation. (Definition based on ISO Guide 73 and NIST SP 800-60 Vol. 1 Rev. 1)

- *Cybersecurity vulnerability* means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

- Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- *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.

- Encryption. The cryptographic transformation of data to produce ciphertext.

- *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.

- Code. System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length.

- *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.

- Exploitable channel. Channel that allows the violation of the security policy governing an information system and is usable or detectable by subjects external to the trusted computing base.

- *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.

- Firmware. Computer programs and associated data 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.

- Hardware. The material physical components of an information system. See firmware and software.

- *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.

- Human-machine interface. The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a color graphics display running dedicated HMI software.

- *Information System* means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software data, applications, communications, and people. It includes the

application of Information Technology, Operational Technology, or a combination of both.

- Information system. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

- *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.

- Information technology product. A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.

- *Known Exploited Vulnerability*, or KEV, means a computer vulnerability that has been exploited in the past.

- Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- *Multi-factor Authentication* means a layered approach to securing data and applications where a system requires users to present a combination of two or more credentials to verify their identity for login.

- Multi-factor authentication. The means used to confirm the identity of a user, process, or device (e.g., user password or token).

- *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. Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

- *Network map* means a visual representation of internal network topologies and components.

- Network map. No comparable NIST definition.

- *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.

- Network segmentation. No comparable NIST definition.

- *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.

- Operational Technology. Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms.

- *Patching* means updating software and operating systems to address cybersecurity vulnerabilities within a program or product.

- Patching. The act of applying a change to installed software—such as firmware, operating systems, or applications—that corrects security or functionality problems or adds new capabilities.

- *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.

- Penetration testing. A method of testing where testers target individual binary components or the application as a whole to determine whether intra or intercomponent vulnerabilities can be exploited to compromise the application, its data, or its environment[al] resources.

- *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.

- Least privilege. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

- *Privileged user* means a user who is authorized (and, therefore, trusted) to perform security functions that ordinary users are not authorized to perform.

- Privileged user. A user [who] is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

- *Risk* means a measure of the extent to which an entity is threatened by a potential circumstance or event and typically is a function of: (1) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

- Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.]

- *Software* means a set of instructions, data, or programs used to operate a computer and execute specific tasks.

- Software. Computer programs and data stored in hardware—typically in read-only memory (ROM) or programmable read-only memory (PROM)—such that the programs and data cannot be dynamically written or modified during execution of the programs.

- *Supply chain* means a system of organizations, people, activities, information, and resources for creating computer products and offering IT services to their customers.

- Supply chain. [A] [l]inked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.

- *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.

- Threat. Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat source to successfully exploit a particular information system vulnerability.

- *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. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- *Vulnerability scan* means a technique used to identify hosts or host attributes and associated vulnerabilities.

- Vulnerability scanning. A technique used to identify hosts/host attributes and associated vulnerabilities.