



May 20, 2024

United States Coast Guard
Office of Port and Facility Compliance
United States Coast Guard Headquarters
2703 Martin Luther King Avenue, SE
Washington, D.C. 20593-7501

RE: Notice of Proposed Rulemaking – Cybersecurity in the Marine Transportation System (Docket No. USCG–2022–0802)

The American Fuel & Petrochemical Manufacturers (AFPM), the International Liquid Terminals Association (ILTA), and The Fertilizer Institute (TFI) (hereinafter, Associations) submit these comments responding to the *Cybersecurity in the Marine Transportation System* Notice of Proposed Rulemaking (NPRM) published by the U.S. Coast Guard (USCG) in the *Federal Register* on February 22, 2024. ILTA represents 82 commercial operators of over 600 aboveground liquid storage terminals that handle a wide range of liquid commodities, including crude oil, refined petroleum products, chemicals, fertilizers, animal fats, and vegetable oils. AFPM is a national trade association whose members comprise virtually all U.S. refining and petrochemical manufacturing capacity. TFI is the voice of the fertilizer industry, representing the public policy, communication, stewardship and sustainability, and market intelligence needs of fertilizer producers, wholesalers, and retailers as well as the businesses that support them with goods and services.

Collectively, the Associations represent the owners and operators of *at least* 750 Maritime Transportation Security Act (MTSA)-regulated facilities in practically every Captain of the Port (COTP) Sector in the United States. For this reason, MTSA requirements are of special interest to the Associations, and these comments focus exclusively on proposed 33 CFR §§ 101.600-670 (hereinafter, Subpart F) relative to facilities subject to 33 CFR Part 105.

I. PERFORMANCE-BASED RULEMAKING: 89 FED. REG. 13,408

COMMENT – THE USCG HAS GENERALLY FOLLOWED A PERFORMANCE-BASED RULEMAKING MODEL FOR SUBPART F.

RECOMMENDATION – THE USCG SHOULD AVOID PRESCRIPTIVE REQUIREMENTS WHILE PROVIDING MAXIMUM REGULATORY FLEXIBILITY.

There is no “one size fits all” cybersecurity program, and the USCG should continue to apply performance-based rulemaking for Subpart F. The USCG has generally committed to proposed rules that are performance-based and adaptable:

This proposed rule would expand upon the agency’s prior actions by establishing minimum *performance-based* cybersecurity requirements for the [Marine Transportation System (MTS)] within the MTSA regulations. Similar to the existing requirements in 33 CFR parts 104, 105 and 106, the Coast Guard would allow owners and operators the

flexibility to determine the best way to implement and comply with these new requirements.

See 89 Fed. Reg. at 13,404, 13,408 (Feb. 22, 2024) (emphasis added).

The Associations strongly support this statement and urge the USCG to maintain maximum regulatory flexibility. The Transportation Security Administration’s (TSA’s) attempt to prescribe pipeline cybersecurity standards offers a cautionary lesson. In July 2021, TSA issued its first Security Directive (SD), which was prescriptive and rigid. Following industry concern, TSA realized that its strict regulatory model was neither sustainable nor appropriate. The agency changed course in July 2022 and stated the following:

TSA has significantly revised the [SD] initially issued in July 2021 to provide Owner/Operators with more flexibility to meet the intended security outcomes while ensuring sustainment of the cybersecurity enhancements accomplished through this [SD] series... This revision also reflects industry feedback along with both industry and general congressional support for TSA’s transition to this performance-based, security outcome model.

Security Directive Pipeline-2021-02C (July 27, 2022), at 2.

The USCG is wise to apply this lesson learned from TSA in the context of the USCG’s cybersecurity rulemaking without exception and should review and realign any prescriptive requirements with the commitment to flexibility stated in the preamble. *See* Comments and Recommendation: Various Sections of 33 CFR § 101.650, *infra*. For example, the proposed *requirement* for penetration testing is unnecessarily prescriptive because a penetration test is only one way, among others, to assess vulnerability. The Associations believe that facilities should have flexibility to choose a penetration test, *or other equivalent means*, to achieve the required outcome.

COMMENT – MANY FACILITIES MUST COMPLY WITH TSA’S SDs THAT MEET OR EXCEED SUBPART F REQUIREMENTS.

RECOMMENDATION – THE USCG SHOULD EXEMPT FACILITIES SUBJECT TO, AND IN COMPLIANCE WITH, TSA’S PIPELINE SDs.

To promote regulatory harmonization, reduce duplication of effort, and preserve resources, the USCG should exempt facilities subject to, and in compliance with, TSA’s SD Pipeline-2021-02 series *Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing* from Subpart F. Like the USCG’s proposed cybersecurity requirements in the maritime domain, the goal of TSA’s SDs “...is to reduce the risk that cybersecurity threats pose to critical pipeline systems and facilities by implementing layered cybersecurity measures that demonstrate a defense-in-depth approach against such threats.” Security Directive Pipeline-2021-02D (July 27, 2023), at 2.

TSA’s SDs require affected facilities to implement and maintain many cybersecurity procedures and measures that meet – and in some cases exceed – those in Subpart F, including:

- Appointing a Cybersecurity Coordinator;
- Reporting significant cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA);

- Developing and executing a TSA-approved Cybersecurity Implementation Plan that outlines the cybersecurity measures the owner/operator maintains to satisfy the SDs, which must, among other things, include network segmentation policies, access control measures, continuous monitoring measures, and measures to reduce the risk of exploitation of unpatched systems;
- Establishing and maintaining a Cybersecurity Incident Response Plan that describes how the owner/operator responds when cybersecurity incidents lead to significant operational interruptions (and which requires testing of at least two objectives each year); and
- Creating a Cybersecurity Assessment Plan that must be updated and re-submitted to TSA annually.

The USCG itself “...emphasizes its commitment to regulatory harmonization and streamlining...” while also acknowledging “...the ongoing rulemakings of other [Department of Homeland Security] (DHS) components, including ongoing rulemakings on cybersecurity in surface transportation modes.” 89 Fed. Reg. at 13,415. Exempting facilities subject to, and in compliance with, TSA’s SDs furthers this goal.

The USCG suggests that proposed 33 CFR § 101.665 on Noncompliance, Waivers, and Equivalents “...could offer stakeholders an option for requesting compliance that is harmonized with similar requirements,” but nearly 20 years of MTA experience has shown this process to be cumbersome, time-consuming, and uncertain. *Id.* The comprehensive nature and overlapping requirements between the SDs and Subpart F suggest a better approach: the USCG should consider an inter-agency Memorandum of Understanding (MOU) with TSA that clarifies regulatory authorities and reduces duplication. Specifically, an MOU should permit facilities that are subject to, and in compliance with, the SDs to use SD plans, procedures, and measures to comply with Subpart F so long as the SDs remain in effect and the facility certifies the same. To the extent that the USCG believes there are material differences between this rulemaking and the SDs, the USCG should mandate that facilities implement only those Subpart F requirements not otherwise captured by TSA. *See id.* (stating that the USCG “...notes potential differences in terminology and policy as compared to those rulemakings.”).

There is precedent between DHS components and different executive departments in this context. In February 2020, for example, DHS and the Department of Transportation (DOT) executed an Annex to a 2004 MOU “...to delineate clear lines of authority and responsibility and promote communications, efficiency, and non-duplication of effort through cooperation and collaboration between the parties in the areas of transportation security and safety based on existing legal authorities and core competencies.” *Annex to the Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation Concerning Transportation Security Administration and Pipeline and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety* [February 26, 2020] (2020) (emphasis added). The USCG can enhance efficiency and reduce duplication of effort by utilizing an MOU model here.

II. APPLICABILITY: 33 CFR § 101.605

COMMENT – FACILITIES WITH LOW CYBERSECURITY RISK WILL BE REQUIRED TO IMPLEMENT COSTLY AND UNNECESSARY CYBERSECURITY MEASURES.

RECOMMENDATION – THE USCG SHOULD BASE SUBPART F APPLICABILITY ON TRANSPORTATION SECURITY INCIDENT (TSI) RISK.

The USCG should consider TSI risk when determining Subpart F applicability among facilities. As drafted, proposed 33 CFR § 101.605 applies Subpart F equally to *all* facilities – even though facilities may have virtually no cyber component outside of email, transfer only low risk commodities (e.g., grain, aggregate, etc.), and/or exclusively employ manual processes for cargo control (e.g., valves are physically

opened, pumps are physically started, etc.). Does a facility transferring Certain Dangerous Cargo (CDC), utilizing complex process control systems in a sophisticated Information Technology (IT) and Operational Technology (OT) environment, have the same TSI risk as a facility transferring woodchips? It does not. Yet, the USCG’s one-size-fits-all approach to applicability means that it proposes to treat CDCs like woodchips while ignoring the fact that TSI risk is a function of threat, vulnerability, and consequence.

Employing a risk-based approach to applicability advances the USCG’s stated purpose “...to safeguard the [M]arine [T]ransportation [S]ystem (MTS) against current and emerging threats associated with cybersecurity by adding minimum cybersecurity requirements ... to help detect, respond to, and recover from cybersecurity *risks* that may cause ... TSIs.” 89 Fed. Reg. at 13,405 (emphasis added). For example, while all facilities may be required to conduct a Cybersecurity Assessment, as proposed in 33 CFR § 101.650(e)(1), a facility that demonstrates a low cybersecurity risk would not implement all proposed Subpart F requirements. Low cybersecurity risk, for example, could be a function of the commodity transferred with a marine vessel, the commodities located inside the facility’s MTSA operating boundary, the exclusive use of manual processes, or maintaining completely air-gapped systems.

Alternatively, the USCG could establish standardized risk criteria. Among other criteria, facilities that transfer CDCs, or have cyber systems connected to their marine cargo systems, for instance, would fall into a “high cybersecurity risk” tier. These facilities would be required to implement all Subpart F cybersecurity measures. Other facilities would fall into a “low cybersecurity risk” or “medium cybersecurity risk” tier – and be required to implement Subpart F accordingly. For some requirements, such as cybersecurity training or reporting, the USCG could require all facilities to apply such measures equally.

This would align to the risk-based approach the USCG employs in other MTSA contexts. For instance, recognizing low TSI risk for facilities transferring only asphalt, the USCG states that “[a]sphalt transfer and storage are low risk operations. If asphalt storage tanks were to be attacked it is unlikely there would be significant loss of life, damage to the environment, significant disruption to the transportation system or to the area’s economy.” Policy Advisory Council 09-09 (Change 1), *Waiving Facilities That Transfer and Store Asphalt*. The USCG also utilized risk-based criteria in its 2016 Transportation Worker Identification Credential (TWIC) Reader Rule by proposing to require only “Risk Group A” facilities that handle CDC to conduct electronic TWIC inspections. The Associations believe the USCG should take a similar risk-based approach here.

III. DEFINITIONS: 33 CFR § 101.615

COMMENT – THE ASSOCIATIONS SUPPORT DEFINING “REPORTABLE CYBER INCIDENT” BUT BELIEVE THE USCG’S PROPOSED DEFINITION IS TOO BROAD.

RECOMMENDATION – THE USCG SHOULD NARROWLY TAILOR “REPORTABLE CYBER INCIDENT” TO ALIGN WITH THE USCG’S MISSION AND THE UNDERLYING PURPOSE OF MTSA.

The Associations support the inclusion of the term “reportable cyber incident” to assist facilities in determining which cybersecurity incidents are reportable – and which are not. However, the USCG’s proposed definition, which is based on the Cyber Incident Reporting Council’s (CIRC’s) model definition from DHS’s September 19, 2023 Report to Congress on cyber incident reporting harmonization, is not narrowly tailored. The proposed definition, if adopted, neither aligns to the USCG’s maritime focus nor MTSA’s underlying purpose, which is to prevent or mitigate a TSI:

[A]n incident that leads to, or, if still under investigation, could reasonably lead to any of the following:

- (1) Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system;*
- (2) Disruption or significant adverse impact on the reporting entity’s ability to engage in business operations or deliver goods or services, including those that have a 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.*

See 89 Fed. Reg. at 13,409.

This definition is too broad and will result in numerous unnecessary reports. For example, while the “[d]isclosure or unauthorized access directly or indirectly of non-public personal information of a significant number of individuals” is an incident that may have legal and financial repercussions for an owner or operator, it would not threaten the MTS, the security of an individual facility, or lead to a TSI.

The definition should be narrowly tailored to either cyber incidents with a direct MTS nexus or cyber incidents that could otherwise result in a TSI. Indeed, the DHS Report to Congress noted flexibility and “mission responsibilities” and stated that “[i]n adopting this model definition, Federal agencies may choose to incorporate some or all the sub-elements based on their authorities and specific mission responsibilities.” DHS Office of Strategy, *Policy, and Plans, Harmonization of Cyber Incident Reporting to the Federal Government* (Sept. 19, 2023), at 26.

The Associations suggest the following definition:

A cyber intrusion, attack, incident, or breach that leads to, or, if still under investigation, could reasonably lead to any of the following:

- (1) Substantial loss of confidentiality, integrity, or availability of an information system, network, or OT system linked to the MTS or that could otherwise result in a TSI;*
- (2) A disruption or significant adverse impact on the MTSA-regulated entity’s ability to engage in business operations or deliver goods or services;*
- (3) The potential operational disruption to critical infrastructure systems or assets linked to the MTS or that could otherwise result in a TSI; or*
- (4) Any other incidents that may lead to a TSI, as defined in 33 CFR 101.105.*

Adopting a mission-focused definition, such as that described above, would increase the security value of the information reported. To provide further specificity, the USCG should also provide examples because terms such as “substantial loss” or “significant adverse impact” would vary.

IV. CYBERSECURITY OFFICER (CYSO): 33 CFR § 101.625

COMMENT – THE ASSOCIATIONS SUPPORT THE FLEXIBILITY PROVIDED IN PROPOSED 33 CFR § 101.625 FOR THE CySO BUT NOTE THAT THE CySO ROLE WILL BE FULFILLED AT THE CORPORATE LEVEL AMONG MANY MTSA FACILITIES.

RECOMMENDATION – THE USCG SHOULD MAINTAIN THE FLEXIBILITY PROVIDED IN PROPOSED 33 CFR § 101.625(a)-(c) FOR THE CySO BUT ACKNOWLEDGE IN THE PREAMBLE AND/OR REGULATION THAT THE CySO ROLE MAY BE FULFILLED AT THE CORPORATE LEVEL.

The Associations support the adaptable and performance-based nature of CySO requirements in proposed 33 CFR § 101.625(a)-(c) and suggest that the USCG maintain the regulatory text, as drafted. Unlike the Facility Security Officer (FSO), who works at the actual MTSA-regulated facility and almost always is a facility-based employee, a CySO likely will serve at the corporate level and could represent many facilities within a company that has multiple MTSA-regulated locations. While this is implied in proposed 33 CFR § 101.625(b) under the heading “Serving as CySO for Multiple Vessels, Facilities, or [Outer Continental Shelf] (OCS) Facilities,” the Associations ask that the USCG expressly acknowledge that a CySO likely will serve at the corporate level either in the preamble to the Final Rule and/or in the text of Subpart F.

It is probable that the person designated as the CySO will have other duties within the IT or OT organization, and the USCG correctly acknowledges this in the preamble when it states that “[t]he CySO may be a full-time, *collateral*, or contracted position.” 89 Fed. Reg. at 13,410 (emphasis added). In other words, it is unlikely that a person will perform *only* the role of CySO. The Associations support proposed 33 CFR § 101.625(c) regarding “Assigning Duties Permitted” because delegation of duties will be required by practical necessity: just as an FSO often must assign duties to “control access to the facility” under 33 CFR § 105.255(a)(3) to a contract security guard, the CySO will also assign duties and actions to others, including contractors, but will maintain “ultimate responsibility.”

COMMENT – MANY REGULATED FACILITIES WILL IDENTIFY AN ALTERNATE CySO.

RECOMMENDATION – THE USCG SHOULD RECOGNIZE THAT A FACILITY MAY DESIGNATE AN ALTERNATE CySO IN PROPOSED 33 CFR § 101.620(b)(3).

While there is no requirement in 33 CFR § 105.200, most facilities have at least one Alternate FSO listed in their Facility Security Plans (FSPs), and the Associations expect that facilities will apply the same reasoning in the context of the CySO as a logical outgrowth of nearly 20 years of FSO experience. For companies operating dozens of facilities, in particular, it is unlikely that a single CySO would possess not only the technical knowledge but also the practical knowledge of each affected facility. This, in turn, will require Alternate CySOs, by necessity. The USCG should acknowledge the same and add the following italicized text to 33 CFR § 101.620(b)(3):

Designate, in writing, by name and by title, a CySO (*and one or more Alternate CySO(s), as necessary*) who is accessible to the Coast Guard 24 hours a day, 7 days a week, and identify how the CySO(s) can be contacted at any time.

The USCG should explain in the preamble that designating an Alternate CySO is not a regulatory requirement. It is a discretionary role, and any person designated as such would have the same: (1) responsibilities listed in proposed 33 CFR § 101.625(d) when the CySO is not available to execute the required duties; and (2) qualifications listed in proposed 33 CFR § 101.625(e).

COMMENT – THE ASSOCIATIONS SUPPORT THE INCLUSION OF THE PHRASE “OR EQUIVALENT JOB EXPERIENCE” IN THE CONTEXT OF CySO QUALIFICATIONS AND THEIR PERFORMANCE-BASED NATURE.

RECOMMENDATION – THE USCG SHOULD MAINTAIN THE PERFORMANCE-BASED, QUALIFICATION FLEXIBILITY PROVIDED IN PROPOSED 33 CFR § 101.625(e).

The Associations support the inclusion of the phrase “or equivalent job experience” and suggest that the USCG maintain this language in the Final Rule. Some CySOs may have formal training or education in the categories listed in proposed 33 CFR § 101.625(e)(1)-(12). Other CySOs will default to, and rely on, “equivalent job experience” to meet some or all qualifications. This mirrors the longstanding approach to certain FSO qualifications. *See* 33 CFR § 105.205(b)(1) (stating that “[t]he FSO must have general knowledge, through training or *equivalent job experience*, in the following...”) (emphasis added).

The Associations also note that the qualifications are performance-based, and the USCG (correctly) does not impose a “CySO litmus-test” in this context. The Associations agree the qualifications must remain performance-based (training or experience), but the proposed provision should be revised to make clear that an owner or operator determines, in accordance with proposed 33 CFR § 101.620(b)(3), whether the CySO meets the requirements in proposed 33 CFR § 101.625(e)(1)-(12). This has longstanding precedent in the context of the Facility Security Rule, where the owner or operator designates the FSO and, in doing so, ensures the FSO satisfies 33 CFR § 105.205(b). *See* 33 CFR § 105.200(b)(2) (stating that the “... *owner or operator* must ... [d]esignate, in writing, by name or by title, a[n] ... FSO and identify how the officer can be contacted at any time.”) (emphasis added).

V. PROTECTING SENSITIVE SECURITY INFORMATION (SSI): 33 CFR § 101.630(B)

COMMENT – SSI IS NECESSARY, BUT NOT SUFFICIENT, TO PREVENT THE RISK OF INADVERTENT OR TARGETED CYBERSECURITY PLAN DISCLOSURE WHEN IN POSSESSION OF THE USCG.

RECOMMENDATION – THE USCG SHOULD CONSIDER ADDITIONAL INFORMATION PROTECTION PROTOCOLS AND INTERNAL CONTROLS.

The Associations express strong concern regarding the risk of inadvertent or targeted disclosure of Cybersecurity Plans when in the possession of the USCG, and, for this reason, the USCG should consider enhanced information protection protocols. Unlike an FSP describing inspection rates, acceptable identification, and vessel deliveries (which are largely the same from facility-to-facility and are either readily known or easily observable), a Cybersecurity Plan will represent a *single-source, detailed roadmap* describing vulnerabilities and protective measures unique to the IT and OT environment for the affected facility. Classifying the Cybersecurity Plan as SSI is necessary, but not sufficient, to ensure that the USCG employs strong internal information security controls and limits access and review only to those with a “need to know.”

The possibility that this document could be released, either inadvertently or intentionally, when in USCG possession is not theoretical. As discussed *infra*, the USCG has misplaced or lost FSPs, and even CISA information systems were compromised recently. *See* Ivanti-Linked Breach of CISA Potentially Affected More Than 100,000 Individuals, Tim Starks (March 29, 2024), <https://cyberscoop.com/ivanti-linked-breach-of-cisa-potentially-affected-more-than-100000-individuals>.

Even if the USCG were to deploy cybersecurity measures equal to those it requires of the regulated community, the risk of inadvertent disclosure remains. Therefore, the Associations suggest that the USCG limit document submissions only to the most basic program documents. Records that, if disclosed, would compromise facility cybersecurity should be maintained at the site as SSI and made available to the USCG for in-person inspection.

VI. CYBERSECURITY PLAN SUBMISSION AND APPROVAL: 33 CFR § 101.630(D)

COMMENT – THE PROPOSED PROCESS FOR CYBERSECURITY PLAN SUBMISSION AND APPROVAL WILL RESULT IN INCONSISTENT OUTCOMES, FORESEEABLE DELAYS, AND ADDITIONAL EFFORT.

RECOMMENDATION – THE USCG SHOULD ESTABLISH A CENTRALIZED CENTER OF EXPERTISE, SUCH AS THE MARINE SAFETY CENTER (MSC), TO REVIEW CYBERSECURITY PLANS.

The Associations urge the USCG to establish a centralized Center of Expertise to conduct Cybersecurity Plan reviews. Establishing a Center of Expertise to serve as the centralized clearinghouse offers several benefits:

1. A Center of Expertise ensures that the USCG uses a consistent framework to review each Cybersecurity Plan submission. Consistency requires not only proper application of the regulation but also application of future, to-be-published guidance. The Associations expect that the Office of Port and Facility Compliance (CG-FAC) will publish a Cybersecurity Plan – Navigation and Vessel Inspection Circular (NVIC) Subpart F Job Aid, or similar guidance materials. These documents will likely provide additional direction and clarification to USCG personnel and affected facilities on regulatory implementation and intent across Subpart F, including Cybersecurity Plan review and approval. USCG personnel assigned to review Cybersecurity Plans will rely on CG-FAC produced documents – and apply deference to them. The Associations base their assumption on nearly 20 years of practice and precedent with MTSA compliance (e.g., NVIC 03-03, Change 2 for the Facility Security Rule and FSPs, and NVIC 03-07 for TWIC implementation).

Consistency is especially important because many companies have more than one MTSA-regulated facility and will develop a “model” Cybersecurity Plan to use across similarly-situated locations with the same IT, OT, and network infrastructure. The regulated community should expect the *same* outcome when submitting the *same* information for review, regardless of Sector. The Associations have reason to believe that deferring to COTPs for Cybersecurity Plan review will exacerbate inconsistency and lead to significantly different results, *even among identical submissions*.

2. A Center of Expertise, by definition, is staffed by personnel knowledgeable in the topic requiring review. Through no fault of their own, COTPs and their staff do not have the technical background required. Yet, proposed 33 CFR § 101.630(d)(1) suggests that Cybersecurity Plan submissions for facilities will be treated in the same manner, and follow the same review model, as other MTSA-filings: the COTP will delegate review and signature authority to the Prevention Department Head who, in turn, will delegate review to Marine Science Technicians under the direction of department staff. The modest number of Cybersecurity Advisor civilian billets added in recent years to bolster subject matter expertise among COTP staff will be helpful, but not technically or administratively adequate, to support review of the approximately 3,411 Cybersecurity Plan submissions expected by the USCG’s estimates. *See* 89 Fed. Reg. at 13,418 (stating an affected population of “[a]pproximately 1,708 facility owners and operators of approximately 3,411 facilities”).

All parties involved would face a no-win situation. The Cybersecurity Plan, which takes *significant time* and resources to develop, will be reviewed by Sector personnel who are unlikely to have technical IT and OT expertise. *See* 89 Fed. Reg. at 13,423 (stating that “[t]he hour-burden estimates are 100 hours for developing the Cybersecurity Plan (average hour burden)...”). The lack of competency in the complex subject matter will, in turn, increase unnecessary delays and result in the

uneven outcomes noted above (e.g., approval of Cybersecurity Plans that should be denied in whole or in part, or denial of Cybersecurity Plans that should be approved in whole or in part).

3. A Center of Expertise will equalize capability and technical knowledge between the CySOs who must submit the Cybersecurity Plans and the USCG personnel who must review them. The USCG contemplates that not all Cybersecurity Plans will be approved upon first submission. In proposed 33 CFR § 101.630(d)(1)(ii), the USCG may “[r]equire 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.” The need for revision or additional information will fall to the CySO, who in turn may require technical dialogue with the Sector personnel who raised the concern in the first instance. Skilled staff at a Center of Expertise are best suited to engage in this context.
4. A Center of Expertise will review submissions in a timelier manner relative to Sector review and is less affected by Sector personnel shortages, Sector personnel rotations, or other emergencies. Because the USCG is understaffed and subject to prioritization of other missions, it routinely takes months for Sector staff to review and return a written decision for an FSP resubmission, even for a mundane amendment. Filings submitted during USCG transfer season, or that must be delayed because of a Sector emergency such as a hurricane, can linger for a year or more. Facilities in Sectors with a high concentration of MTSA-regulated facilities, such as Houston-Galveston, New Orleans, and New York, are likely to face further delays relative to those in Sectors with fewer facilities.
5. A Center of Expertise has precedent in the context of security plan reviews, especially when the subject matter is new or the task is technical. In 2004, the USCG directed a centralized review of FSPs and hired a contractor to assist. Before the July 1, 2004 effective date, the Government Accountability Office (GAO) assessed and summarized the process:

As part of our work in evaluating the process for reviewing security plans, we visited the Coast Guard’s contractors at the [MSC] in Washington, D.C., and the National Facility Security Plan Review Center in Overland Park, Kansas. During these visits, we also talked with contractor management and staff to determine how the review process worked, what reviewers were finding in the plans during their reviews, how deficient plans were dealt with, *and what internal controls and quality assurance mechanisms were in place to ensure consistency during the review process.*

GAO Report 04-838, *Maritime Security, Substantial Work Remains to Translate New Planning Requirements into Effective Port Security* (June 2004), at 36 (emphasis added).

The importance of a consistent, centralized approach for Cybersecurity Plan review, with mechanisms for quality control, cannot be overstated and is more relevant in 2024 than in 2004. Cybersecurity subject matter is more complex than physical security subject matter, and the USCG’s expectations are just as high. *See* 89 Fed. Reg. at 13,423 (stating that “[w]hile the Cybersecurity Plan can be incorporated into an existing FSP..., this does not mean that the Cybersecurity Plan is expected to be less complex to develop or maintain than an FSP. In general, the provisions outlined in this proposed rule are meant to reflect the depth and scope of the physical security provisions established by MTSA.”). Perhaps for these and other reasons, the USCG will continue to centralize Vessel Security Plan reviews at the MSC and should also do so for Cybersecurity Plans submitted by facilities. *See* proposed 33 CFR § 101.630(d) (stating that “[e]ach owner or operator must submit one copy of their Cybersecurity Plan for review and approval ... to the MSC for the vessel.”).

Experience with NVIC 01-20, *Guidelines for Addressing Cyber Risks at [MTSA] Regulated Facilities*, informs this comment. The Associations’ members collectively submitted *hundreds* of NVIC 01-20 appendices for USCG review and approval. Facilities experienced a lack of technical understanding and divergent outcomes from Sector to Sector, and even within the *same* Sector: companies that submitted the *same* NVIC 01-20 cybersecurity appendix for facilities located in different Sectors saw one Sector approve the document, but another Sector reject it. Some Sectors required facilities to include at least one “cyber risk” in their Form CG-6025 while others did not. Even though CG-FAC issued a 14-page NVIC 01-20 Job Aid in March 2020, followed by an eight-page revised Job Aid in January 2023, at least one Sector invented its own one-page “rogue” Job Aid around October 2021. History should not repeat itself.

COMMENT – THE ASSOCIATIONS SUPPORT PROPOSED 33 CFR § 101.630(d)(2) PERMITTING ONE CYBERSECURITY PLAN TO COVER TWO OR MORE FACILITIES OF SIMILAR OPERATIONS.

RECOMMENDATION – THE USCG SHOULD MAINTAIN THE PRAGMATIC APPROACH IN PROPOSED 33 CFR § 101.630(d)(2) BECAUSE COMPANIES WITH MULTIPLE FACILITIES SEEK ECONOMIES OF SCALE AMONG SIMILARLY-SITUATED OPERATIONS.

The Associations strongly support proposed 33 CFR § 101.630(d)(2) because most of the Associations’ member companies have more than one MTSA facility – and some have 30 or more MTSA facilities. These companies manage cybersecurity as a corporate function using a hub-and-spoke model: IT and OT cybersecurity personnel assess, develop, implement, and maintain IT and OT cybersecurity practices centrally, and then distribute them locally. Among facilities of the same or similar operation within a single enterprise, a facility in Sector Miami generally will have the same cybersecurity measures – and risks – as another facility in Sector San Francisco. Risks that are unique at one facility relative to another receive different or additional cybersecurity measures, as needed, and the Associations agree that “...the Plan [should address] the specific cybersecurity risks for each ... facility” when variations exist. \

VII. CYBERSECURITY PLAN AMENDMENTS: 33 CFR § 101.630(E)

COMMENT – THE PROPOSED CYBERSECURITY PLAN AMENDMENT PROCESS MAY RESULT IN FACILITIES REMAINING UNNECESSARILY EXPOSED TO CYBERSECURITY THREATS.

RECOMMENDATION – THE USCG SHOULD REVISE THE PROPOSED CYBERSECURITY PLAN AMENDMENT AND APPROVAL PROCESS TO ALLOW FACILITIES TO IMMEDIATELY IMPLEMENT CRITICAL CYBERSECURITY MEASURES WHEN MADE DIRECTLY IN RESPONSE TO AN EMERGING CYBERSECURITY THREAT.

The USCG should modify proposed 33 CFR § 101.630(e)(2) because it will prevent facilities from implementing new or different cybersecurity measures to counter an immediate or novel threat. Unlike the physical risk environment, which has generally remained static for years, cybersecurity risk changes rapidly. The USCG correctly acknowledged this fact when it stated that “...cybersecurity threats require the maritime community to effectively manage *constantly changing risks*.” 89 Fed. Reg. at 13,405 (emphasis added). Proposed 33 CFR § 101.630(e)(2) hampers a facility’s response to “constantly changing risk” because “[m]ajor amendments ... to the Cybersecurity Plan must be proposed to the Coast Guard *prior to implementation*[]” and the proposed amendment “...must be sent to the Coast Guard *at least 30 days before the proposed amendment’s effective date*.” (emphasis added).

However, an emerging threat may require a facility to implement a new or materially different cybersecurity measure(s) as a “major amendment.” Before it could do so, the facility would need to update and submit its Cybersecurity Plan to the USCG at least 30 days prior to implementing the measure(s). The plain reading of the text suggests that no further risk mitigation action could occur until *after* the USCG grants amendment approval. Given longstanding Sector delays for basic FSP physical security amendment reviews, the Associations believe that cybersecurity amendment reviews will suffer the same fate and take months (or longer). This outcome runs counter to Subpart F’s stated purpose.

The Associations urge the USCG to permit facilities to *immediately* implement critical cybersecurity measures – even if they constitute a “major amendment” – when made *directly* in response to an emerging cybersecurity threat following notice to the USCG. This should be accomplished by adding the following text to the end of proposed 33 CFR § 101.630(e)(2):

If a proposed amendment in accordance with this part is required to address an exigent cybersecurity risk, then the owner or operator may implement the proposed amendment to the extent necessary to mitigate the risk after providing notice to the Coast Guard.

VIII. CYBERSECURITY PLAN AUDITS: 33 CFR § 101.630(F)

COMMENT – SUBPART F INCLUDES CONFLICTING STATEMENTS REGARDING CYBERSECURITY PLAN AUDITS.

RECOMMENDATION – THE USCG SHOULD DECONFLICT THE REQUIREMENT THAT THE CySO MUST CONDUCT THE CYBERSECURITY PLAN AUDIT FROM THE AUDITOR INDEPENDENCE REQUIREMENT.

The USCG should deconflict proposed regulatory provisions mandating the CySO to conduct a Cybersecurity Plan audit from the requirement for auditor independence. Proposed 33 CFR § 101.630(f)(2) states that “...the CySO must audit the Cybersecurity Plan if there is a change in the owner or operator ... or if there have been modifications to the cybersecurity measures...” The Associations note that this language is similar to 33 CFR § 105.415(b)(2) for FSP audits, but the USCG modified the proposed text to make *the CySO* the auditor. Compare 33 CFR § 105.415(b)(2) (stating “[t]he FSP must be audited...”) with proposed 33 CFR § 101.630(f)(2) (stating “...*the CySO* must audit the Cybersecurity Plan...”) (emphasis added).

Proposed 33 CFR § 101.630(f)(4)(ii)-(iii) then establishes qualifiers for Cybersecurity Plan auditors. The auditors cannot “...have regularly assigned cybersecurity duties for the ... facility ... being audited” and must “[b]e independent of any cybersecurity measures being audited.” These requirements conflict because CySOs, or their assignees under proposed 33 CFR § 101.625(c), will have regularly assigned cybersecurity duties and cannot be independent of the cybersecurity measures being audited. The USCG should modify the beginning of proposed 33 CFR § 101.630(f)(2) with the following text:

In addition to the annual audit, the Cybersecurity Plan must be audited if there is a change in the owner or operator of the vessel, facility, or OCS facility...

COMMENT – THE REQUIREMENT TO AUDIT THE CYBERSECURITY PLAN FOLLOWING “MODIFICATIONS TO CYBERSECURITY MEASURES” IS TOO BROAD.

RECOMMENDATION – THE USCG SHOULD NARROWLY TAILOR THE REGULATORY TEXT TO REQUIRE AUDITS AS A RESULT OF “MATERIAL” OR “SIGNIFICANT” MODIFICATIONS TO CYBERSECURITY MEASURES.

The USCG should define the phrase “modifications to cybersecurity measures” in proposed 33 CFR § 101.630(f)(2). The regulatory text is likely to result in *multiple* audits of discrete Cybersecurity Plan sections each year. Modifications “...including, but not limited to, physical access, incident response procedures, security measures, or operations” *should be expected* among facilities with Cyber Risk Management (CRM)-informed IT and OT security programs. Indeed, the USCG, itself, does not expect facilities to remain idle in response to cybersecurity changes and new threats. *See* 89 Fed. Reg. at 13,407 (stating that “[m]aritime stakeholders can better detect, respond to, and recover from cybersecurity risks that may cause TSIs by adopting a range of [CRM] measures, as described in this proposed rule.”).

The USCG should narrowly tailor this provision to require Cybersecurity Plan audits only following “material” or “significant” modifications, as determined by the CySO. This approach would align with the flexibility afforded to amendments. Proposed 33 CFR § 101.630(e)(2) only requires “[m]ajor amendments” to the Cybersecurity Plan to be proposed to the USCG prior to implementation, “...as determined by the owner or operator based on types of changes to their security measures and operational risks...” The same deference and judgment should be afforded here in the context of cybersecurity measures. Proposed 33 CFR § 101.630(f)(3), which limits the audit “...to those sections of the Plan affected by the modifications,” is necessary but not sufficient because it does not affect whether an audit is required in the first place.

IX. CYBERSECURITY EXERCISES: 33 CFR § 101.635(C)

COMMENT – THE ASSOCIATIONS DISAGREE WITH THE USCG’S ASSUMPTION THAT THE PROPOSED ANNUAL CYBERSECURITY EXERCISES WILL NOT REQUIRE ADDITIONAL TIME FROM PARTICIPANTS.

RECOMMENDATION – THE USCG SHOULD ADJUST THE REGULATORY TEXT IN THE FINAL RULE TO ALLOW MORE FLEXIBILITY FOR COMBINING ANNUAL CYBERSECURITY EXERCISES WITH ANNUAL PHYSICAL SECURITY EXERCISES OR INCREASE THE COST ESTIMATE.

The Associations disagree with the USCG’s assumption that the proposed annual cybersecurity exercise will not require additional time from participants. The USCG bases its cost estimates on the assumption “...that owners and operators will hold these new exercises in conjunction with existing [physical security] exercises.” 89 Fed. Reg. 13,430. The USCG then concludes that they “...will not require any additional time from participants, which means that the only new cost associated with the proposed cybersecurity exercises is the development of cybersecurity components to add to existing exercises.” *Id.* This is not correct because the regulatory text describing exercise parameters virtually mirrors the physical security exercise *already required* by 33 CFR Parts 104 – 106. Specifically, proposed 33 CFR § 101.635(c)(4)-(5) states that “[e]ach exercise must *test communication and notification procedures and elements of coordination, resource availability, and response,*” be “...*a full test of the cybersecurity program*[,] and ... include the substantial and active participation of the CySO(s).” (emphasis added). To satisfy both the physical elements and cybersecurity elements in the same setting, a combined exercise would need to test significantly greater subject matter, by definition. This would result in a longer exercise that necessitates additional participant time and preparation time.

The Associations suggest that the USCG either increase its cost estimate or adjust the proposed regulatory language to allow more flexibility for a combined exercise event. In the case of the latter, the USCG should add the following text after 33 CFR § 101.635(c)(6):

(7) If the exercise required by this Part is combined with the exercise required by 33 CFR 104.220(c)(4), 33 CFR 105.220(c)(4), or 33 CFR 106.220(c)(4) in a single event, then the exercise required by this Part must test at least three alternating sections of the Cybersecurity Plan every year.

X. CYBERSECURITY MEASURES: VARIOUS SECTIONS OF 33 CFR § 101.650

THE ASSOCIATIONS MAKE THE FOLLOWING COMMENTS AND CORRESPONDING RECOMMENDATIONS OR OBSERVATIONS REGARDING THE TECHNICAL FEASIBILITY, UTILITY, OR UNINTENDED CONSEQUENCES OF SPECIFIC CYBERSECURITY MEASURES PROPOSED IN 33 CFR § 101.650:

- **Account Security Measures – 33 CFR §101.650(a)(1)** – Proposed 33 CFR § 101.650(a)(1) requires facilities to have “[a]utomatic account lockout after repeated failed login attempts ... enabled on all password-protected IT and OT systems” without consideration of unintended safety or operational risk. As explained in the International Society of Automation’s (ISA’s) / International Electrotechnical Commission’s (IEC’s) widely accepted standards on industrial control system cybersecurity, “[a]ccess controls ... shall not prevent the operation of essential functions, specifically: accounts used for essential functions shall not be locked out, even temporarily.” ISA/IEC-62443-3-3, *System Security Requirements and Security Levels*, at § 4.2. The National Institute of Standards and Technology (NIST) *Guide to Operational Technology Security* echoes ISA / IEC and notes:

A unique challenge in OT is the need for immediate access to a[] [Human Machine Interface] in emergency situations. The time needed to enter a user’s credentials may impede response or intervention by the operator, resulting in negative consequences to safety, health, or the environment.

NIST SP 800-82 Rev. 3, *Guide to Operational Technology Security* (September 28, 2023), at 97.

For these reasons, the USCG should limit forced lockout requirements to password-protected IT systems. With regard to OT systems, when lockouts are not supported or advisable “due to impacts on performance, safety, or reliability...,” NIST suggests organizations “...select compensating countermeasures, such as the use of physical security (e.g., control center keycard access for authorized users) to provide an equivalent security capability or level of protection.” *Id.* The USCG should align its proposed OT-related account security measures with this well-established practice.

- **Device Security Measures – 33 CFR § 101.650(b)(4)** – Without consideration of the information security risk that it creates, proposed 33 CFR § 101.650(b)(4) requires facilities to “[d]evelop and maintain accurate documentation identifying the network map and OT device configuration information.” The network map must be documented in Section 6 of the Cybersecurity Plan. *See* 33 CFR § 101.650(b). To justify this directive, the USCG states that “[t]hese requirements are foundational to many industry consensus standards and would reinforce Coast Guard regulations to protect communication networks.” 89 Fed. Reg. at 13,412.

The USCG should consider the utility of including a network map in the Cybersecurity Plan relative to the risk created. A network map is highly sensitive, and its inclusion in the submitted Cybersecurity

Plan merely to “...reinforce Coast Guard regulations to protect communications networks” offers no compliance benefit. It does, however, increase the possibility that the information is accessed by a person without “a need to know” – or otherwise mismanaged because of poor document control. In the case of the latter, the Associations are aware of several instances where a common carrier requiring delivery signature (e.g., FedEx) successfully delivered an FSP sent by a facility to the USCG, but the USCG lost the FSP following delivery to its office.

The Associations suggest that the USCG update proposed 33 CFR §§ 101.650(b) and (b)(4) with the following italicized text to increase information security of this highly sensitive data:

(b) Device security measures. Each owner or operator or designated CySO of a vessel, facility, or OCS facility must ensure the following device security measures are in place and documented in Section 6 of the Cybersecurity Plan *unless otherwise stated*:

(4) Develop and maintain accurate documentation identifying the network map and OT device configuration information *that can be made available for inspection or examination upon request*.

- **Data Security Measures – 33 CFR § 101.650(c)(2)** – Proposed 33 CFR § 101.650(c)(2) requires “[a]ll data, both in transit and at rest, ... [to] be encrypted using a suitably strong algorithm,” but most OT equipment does not support at-rest data encryption as a threshold matter. The USCG appears to disregard the fact that OT systems rely upon insecure communication protocols to operate (e.g., OPC classic, Modbus TCP, BACnet/IP, DNP, Vnet, etc.) and encryption tunneling would require considerable investment to implement, where even possible. Additionally, OT systems often prioritize availability over confidentiality, and a blanket requirement to implement data encryption in transit and at rest may present an increased risk to OT availability. Encryption within OT environments can cause latency issues for time-sensitive equipment and performance degradation due to the computing power needed to encrypt, decrypt, and authenticate. The Associations suggest that the USCG replace proposed 33 CFR § 101.650(c)(2) with the following text to allow for mitigating countermeasures:

All confidential data in transit and at rest must be encrypted using a suitably strong algorithm. Cybersecurity plans must document mitigating countermeasures where encryption is not technically feasible or presents increased risk to OT system availability, performance, safety, or reliability.

This would align with the allowances for documenting justified device security measure exemptions in Cybersecurity Plans, as specified in proposed 33 CFR § 101.650(b)(2).

- **Cybersecurity Training for Personnel – 33 CFR § 101.650(d)(2)** – The USCG should clarify the phrase “key personnel” for enhanced cybersecurity training to ensure consistent training application. Subpart F proposes new cybersecurity training requirements for two populations: (1) a general cybersecurity training for all personnel with access to the IT or OT systems; and (2) an enhanced cybersecurity training for *key personnel* with access to the IT or remotely accessible OT systems. *See* proposed 33 CFR § 101.650(d)(1)-(2) (emphasis added). Other than noting that “key personnel” include persons with access to remotely accessible OT systems, “key personnel” is not defined.

This will create confusion and inconsistent rule application because there is no objective way to distinguish “key personnel” from the broader population of facility personnel (who do not need additional training). Some facilities may take an unnecessarily broad view of applicability, but other

facilities may take a very narrow view. To avoid this outcome, the USCG should either add “key cybersecurity personnel” to the definitions in proposed 33 CFR § 101.615 or clarify the phrase. The USCG could, for example, characterize “key personnel” as follows:

Persons who (1) possess administrative or management-level privileges for IT or OT systems, or remote ‘read-write’ access to OT systems; or (2) should be deemed “key personnel” based on the person’s IT or OT responsibilities in the discretion of the CySO.

- **Risk Management (Cybersecurity Assessment) – 33 CFR § 101.650(e)(1)(iii)** – The USCG should require facilities to document any recommendations and resolutions in the Cybersecurity Assessment itself – and not in the Facility Security Assessment (FSA). Documenting “...recommendations and resolutions in the [FSA]...in accordance with ...105.305” unnecessarily commingles new Subpart F requirements with existing (and longstanding) 33 CFR § 105.305 provisions. As further described below, 33 CFR § 105.305 *et seq.* has no “cybersecurity” references or requirements, and no other part or subpart of 33 CFR § 101.650 requires reference to, or consideration of, an owner’s or operator’s existing FSP security measures or FSA vulnerabilities. In other words, except for 33 CFR § 101.650(e)(1)(iii), the cybersecurity measures mandated by 33 CFR § 101.650 stand “on their own” in a “self-contained” document. There is no reason for the “recommendations and resolutions” to exist outside of this framework as an exception.

The Associations further assume that Subpart F will supersede and replace 33 CFR §§ 105.305(c)(1)(5) and (d)(2)(v). These provisions, which have existed in MTSA since its inception nearly 20 years ago and form the regulatory basis of NVIC 01-20, direct assessment of “[m]easures to protect radio and telecommunication equipment, *including computer systems and networks*” in FSAs, and description of “[r]adio and telecommunications systems, including computer systems and networks” in FSA Reports. *Id.* (emphasis added). The Associations believe that these specific provisions become unnecessary upon Subpart F’s full implementation, and the USCG should amend 33 CFR Part 105 to strike 33 CFR §§ 105.305(c)(1)(5) and (d)(2)(v) as part of this rulemaking.

- **Risk Management (Penetration Testing) – 33 CFR § 101.650(e)(2)** – Proposed 33 CFR § 101.650(e)(2) requires the owner or operator or designated CySO to ensure that a penetration test is completed “[i]n conjunction with FSP ... renewal.” The Associations believe the USCG made a technical error in the regulatory text by linking the penetration testing requirement with FSP renewal rather than Cybersecurity Plan renewal. The preamble supports this assumption. *See* 89 Fed. Reg. at 13,488 (stating that “[the USCG]...has proposed requiring penetration tests every 5 years, *aligned with the renewal of a Cybersecurity Plan...*”) (emphasis added). The USCG should correct this technical error by adjusting 33 CFR § 101.650(e)(2) to link the penetration testing requirement with Cybersecurity Plan renewal, as follows:

In conjunction with Cybersecurity Plan renewal, the owner or operator or designated CySO must ensure that a penetration test has been completed.

- **Risk Management (Routine System Maintenance) – 33 CFR § 101.650(e)(3)(i)** – Proposed 33 CFR § 101.650(e)(3)(i) requiring “...patching or implementation of documented compensating controls for all [Known Exploited Vulnerabilities (KEVs)] in critical IT or OT systems, without delay” is too prescriptive for a risk-based activity in the OT environment and ignores the reality that OT patches and recommended countermeasures are often unavailable. As stated in the *Dragos OT Cybersecurity 2023 Year in Review* regarding Industrial Control System (ICS)/OT vulnerabilities,

28% had no patches available, 74% had no mitigating countermeasures, and 19% had no patch and no mitigation available. *See Dragos OT Cybersecurity 2023 Year in Review* (February 2024), at 28.

Even when patches are available, they must be approved by the system Original Equipment Manufacturer (OEM) or vendor and need testing before ICS/OT environment deployment. The Associations suggest that the USCG revise proposed 33 CFR § 101.650(e)(3)(i) to remove the word “*all*” and permit a vulnerability management process. Such a process would allow a facility to take credit for alternative security countermeasures when patches and other remediation activities are unavailable, technologically unfeasible, or increase risk to operational safety.

- **Risk Management (Without Delay) – 33 CFR § 101.630(e)(3)-(4) and 33 CFR § 101.650(e)(3)(i), (f)(2), and (g)(1)** – The USCG should define the phrase “without delay” to prevent inconsistent regulatory outcomes and to establish clear reporting expectations. Subpart F uses the “without delay” qualifier to mandate facility action in five proposed regulatory provisions:
 - (1) 33 CFR § 101.630(e)(3): If the owner or operator has changed, the CySO must amend the Cybersecurity Plan, *without delay*, to include the name and contact information of the new owner or operator and submit the affected portion of the Plan for review and approval in accordance with this part.
 - (2) 33 CFR § 101.630(e)(4): If the CySO has changed, the Coast Guard must be notified *without delay* and the affected portion of the Cybersecurity Plan must be amended and submitted to the Coast Guard for review and approval in accordance with this part *without delay*.
 - (3) 33 CFR § 101.650(e)(3)(i): Ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems, *without delay*.
 - (4) 33 CFR § 101.650(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*.
 - (5) 33 CFR § 101.650(g)(1): Report any cyber incidents to the [National Response Center] [(NRC)], *without delay*, to the telephone number listed in § 101.305 of this part.

The MTSA-regulated community recognizes the phrase “without delay” here because it has been part of existing MTSA regulation in the context of incident reporting for nearly 20 years. *See* 33 CFR § 101.305. What “without delay” means (or does not mean) varies widely across Sectors – and even within the same Sector. Under some Sector interpretations over the years, a facility complies with its “without delay” obligations so long as the NRC report is made the same day as the triggering incident. In other Sectors, USCG personnel have questioned why a facility did not make NRC notification less than one hour after the triggering incident. In other examples, facilities choose to define the phrase “without delay” in their FSPs specifically to avoid uncertainty.

The Associations urge the USCG to establish clear timing requirements for each instance where “without delay” is used. For example, a revised proposed 33 CFR § 101.630(e)(3)-(4) might read as follows, with changes noted in italics:

If the owner or operator has changed, the CySO must amend the Cybersecurity Plan *within 7 days of the change* 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.

If the CySO has changed, the Coast Guard must be notified *no more than 24 hours after the change* 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 *within 30 days*.

Similarly, a revised version of the applicable sections of 33 CFR § 101.650 might read as follows, with changes noted in italics:

Ensure patching or implementation of documented compensating controls for all KEVs in critical IT or OT systems *as soon as practicable*.

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 *no more than 8 hours after occurrence or discovery*.

Report any cyber incidents to the NRC to the telephone number listed in § 101.305 of this part *no more than 24 hours after occurrence or discovery*.

It is unclear why the USCG would provide objective timing expectations for cybersecurity training, for example, but would not do so for “without delay.” See 33 CFR § 101.650(d)(3) (stating that, among other things, “[t]raining for new personnel not in place at the time of the effective date of this rule must be completed within [five] days of gaining system access, but no later than within 30 days of hiring, and annually thereafter.”). DHS itself has recommended clarity on when reporting is triggered. See DHS Office of Strategy, Policy, and Plans, *Harmonization of Cyber Incident Reporting to the Federal Government* (Sept. 19, 2023), at 27 (stating that “[f]ederal agencies should align requirements for when entities must file cyber incident reports and identify the “triggers” that elicit such a requirement, i.e., start the clock on the obligation to report consistent with the agency’s need for information.”).

Other DHS transportation security regulations do not make affected entities guess when soon is soon enough, and neither should the USCG. For example, TSA’s Rail Transportation Security Rule requires regulated rail operators to “...report, *within 24 hours of initial discovery*, any potential threats and significant security concerns...” 49 CFR § 1570.203(a)(1) (emphasis added). Similarly, TSA’s SDs mandate that affected pipeline operators report cybersecurity incidents “...as soon as practicable, *but no later than 24 hours after a cybersecurity incident is identified*.” Security Directive Pipeline-2021-01C, at 3. More recently, DHS proposes a 72-hour reporting rule for cyber incident reporting under its Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) Reporting Requirements. See generally, 89 Fed. Reg. at 23,644

- **Supply Chain (Vulnerability Notifications) – 33 CFR § 101.650(f)(2)** – Proposed 33 CFR § 101.650(f)(2) requiring facilities to “[e]stablish 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” is not practical. While owners and operators could include notification provisions in contractual agreements with certain IT and OT vendors (i.e., requiring notification of any known cybersecurity vulnerability within a set number of hours), contract compliance (and enforcement) is less certain.

It is equally unreasonable to expect owners and operators to require notifications from *all* IT and OT vendors: a facility using Microsoft products in its IT environment, for example, cannot demand Microsoft provide cybersecurity vulnerability notifications without delay simply because the facility is subject MTSA. To the contrary, if the facility wants to continue to use Microsoft products, then it is bound by Microsoft’s end-user licensing agreements (and those agreements are non-negotiable for practical purposes). Further, the requirement to notify the owner or operator, or designated CySO, of “*any* cybersecurity vulnerabilities, incidents, or breaches” presupposes that the vendor is aware or has actual knowledge of the vulnerability, incident, or breach. However, vulnerabilities and breaches may not be identified for weeks, months, or longer. A recent IBM report indicated that in 2023, businesses took an average of 204 days to identify a cybersecurity breach. *See IBM Security, Cost of a Data Breach Report 2023*, at 14.

The Associations suggest that the USCG replace proposed 33 CFR § 101.650(f)(2) with the following text which: (1) adds “where possible;” (2) removes “all” before “IT and OT vendors and service providers;” and (3) adds “known” before “cybersecurity vulnerabilities, incidents, or breaches:”

Where possible, establish a process through which IT and OT vendors or service providers notify the owner or operator or designated CySO of any known cybersecurity vulnerabilities, incidents, or breaches....

XI. CYBERSECURITY COMPLIANCE DATES: 33 CFR § 101.655

COMMENT – THE PROPOSED TIMELINE FOR CYBERSECURITY PLAN SUBMISSION IS UNCLEAR AND WILL LEAD TO INCONSISTENT SUBMISSION OUTCOMES AND EXPECTATIONS.

RECOMMENDATION – THE USCG SHOULD CHANGE THE CYBERSECURITY PLAN SUBMISSION TIMELINE TO 24 MONTHS AFTER THE FINAL RULE EFFECTIVE DATE

The proposed timeline for Cybersecurity Plan submissions is unclear on its face and will lead to uncertainty and inconsistent submission outcomes and expectations. Proposed 33 CFR § 101.655 requires “[a]ll Cybersecurity Plans ... [to] be submitted to the Coast Guard for review and approval *during the second annual audit* [of the existing approved FSP] following [EFFECTIVE DATE OF FINAL RULE]....” (emphasis added). In the preamble, the USCG states that the “...Cybersecurity Plan would be *made available to the Coast Guard for review* during the second annual audit of the existing, approved ... FSP...” 89 Fed. Reg. at 13,414 (emphasis added).

The phrase “during the second annual audit” is unclear: does this mean that a facility must submit the Cybersecurity Plan on the actual date of the second annual audit? Further, the USCG’s explanation in the preamble that the Cybersecurity Plan would be “made available to the Coast Guard for review” during the second annual audit incorrectly suggests that facilities would hand the USCG a copy of the Cybersecurity Plan during the second annual FSP audit. The USCG appears to disregard the fact that the FSP audit is an *internal* review conducted by the owner or operator in accordance with 33 CFR § 105.415. The USCG is neither involved nor present, and the annual FSP audit would not be the appropriate time or forum to make the Cybersecurity Plan available to the USCG.

Facilities’ annual FSP audits are scheduled during different times throughout the year and making the Cybersecurity Plan deadline a function of the FSP audit date will yield timing differences and confusion. There could be scenarios where facilities are not technically required to submit their Cybersecurity Plans

to the USCG until two and a half years (or approximately 30 months) *after* the effective date. Consider the following scenario:

- Assume that the Final Rule’s effective date is June 30, 2025.
- Further assume that a facility completes its annual FSP audit on June 15, 2025.
- The facility’s first annual FSP audit following the effective date would occur in or around June 2026.
- The facility’s second annual FSP audit following the effective date would occur in or around June 2027 – but technically could occur as late as December 2027. *See* NVIC 03-03, Change 2, Enclosure 8 (stating that “[o]wners and operators must ensure that audits are performed annually ... with no more than 18 months between audits.”).

This result conflicts with the USCG’s desire for “...an implementation period of 12 to 18 months following the effective date of a [F]inal [R]ule...” and will lead to uneven application of the regulation among companies with more than one affected facility. 89 Fed. Reg. at 13,408. The Associations support the USCG’s intent “...to allow adequate time for owners and operators to develop a Cybersecurity Plan,” but ask the USCG to provide a clear submission timeline and update proposed 33 CFR § 101.655 with the following italicized text:

All Cybersecurity Plans mentioned in this subpart must be submitted to the Coast Guard for review and approval *no later than 24 months* following [EFFECTIVE DATE OF FINAL RULE], according to 33 CFR 104.415 for vessels, 33 CFR 105.415 for facilities, or 106.415 for OCS facilities.

XII. CANCELLATION OF NVIC 01-20

COMMENT – WHILE THE ASSOCIATIONS ASSUME THAT SUBPART F WILL SUPERSEDE NVIC 01-20, THIS IS NOT EXPRESSLY STATED IN THE REGULATORY TEXT OR PREAMBLE.

RECOMMENDATION – THE USCG SHOULD CLARIFY THAT SUBPART F WILL SUPERSEDE NVIC 01-20.

The Associations assume that when Subpart F becomes effective, and a separate Cybersecurity Plan is approved by the USCG, Subpart F will supersede NVIC 01-20, *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act Regulated Facilities*, but this is not clear. To comply with NVIC 01-20, facilities either incorporated cybersecurity measures into individual sections of their FSPs or developed cybersecurity appendices that are now attached to their FSPs. In either case, Subpart F’s requirements far exceed NVIC 01-20 and expressly add cybersecurity requirements to 33 CFR Part 101.

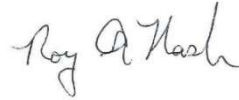
The USCG generally provides such clarification when an important policy document is replaced. For instance, NVIC 02-24, *Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents*, published in February 2024, notes that the USCG’s previous guidance on the subject is no longer in effect. *See* NVIC 02-24 (February 21, 2024), at 2 (stating “CG-5P Policy Letter 08-16 is hereby cancelled.”). The Associations request that the USCG provide similar clarification here.

Thank you for the opportunity to comment. Please contact the undersigned with any questions.

Sincerely,



Steven Roberts
Roberts Law Group PLLC
(713) 572-3600
roberts@chemicalsecurity.com



Roy Nash
Nash Maritime Consulting LLC
(703) 943-8865
roy.nash@nashmaritimeconsultingllc.com



Dan Slaton
Roberts Law Group PLLC
(713) 572-3600
slaton@chemicalsecurity.com

Association Representatives



Jeff Gunnulfsen
Senior Director, Security & Risk Management
American Fuel & Petrochemical Manufacturers
(202) 457-0480
jgunnulfsen@afpm.org



Leakhena Swett
President
International Liquid Terminals Association
(703) 851-2938
lswett@ilta.org



Reagan Giesenschlag
Manager, Government Affairs
The Fertilizer Institute
(830) 385-3887
rgiesenschlag@tfi.org