The American Waterways Operators

801 North Quincy Street
Suite 500
Arlington, VA 22203

PHONE: 703.841.9300
EMAIL: jcarpenter@americanwaterways.com

Jennifer A. Carpenter
President & CEO

May 22, 2024

RDML Wayne Arguin
Assistant Commandant for Prevention Policy
U.S. Coast Guard
2703 Martin Luther King Jr. Ave. SE
Washington, DC 20593

Re: Cybersecurity in the Marine Transportation System (Docket No. USCG-2022-0802)

Dear Rear Admiral Arguin:

The American Waterways Operators (AWO) is the tugboat, towboat and barge industry's advocate, resource and united voice for safe, sustainable and efficient transportation on America's waterways, oceans and coasts. Our industry is the largest segment of the nation's 40,000-vessel domestic maritime fleet and moves 665 million tons of cargo each year safely, sustainably and efficiently. On behalf of AWO's more than 300 member companies, we appreciate the opportunity to comment on the U.S. Coast Guard's proposed rule to establish minimum cybersecurity requirements for U.S.-flagged vessels and facilities subject to the Maritime Transportation Security Act of 2002 (MTSA).

For over 20 years, AWO has been committed to working in partnership with the Coast Guard to ensure the security of the marine transportation system. Immediately after September 11, 2001, AWO began working with the Coast Guard and the U.S. Army Corps of Engineers to develop a Model Vessel Security Plan for towing vessels, more than a year before such plans were required by law. When MTSA was enacted in 2002, AWO worked with the Coast Guard to transform the Model Vessel Security Plan into one of the first Coast Guard-approved Alternative Security Programs, and the AWO ASP remains the most widely used ASP in the maritime industry. In 2017, recognizing the potential of cyber-attacks to disrupt the continuity of maritime commerce, the Coast Guard-AWO Safety Partnership National Quality Steering Committee established a Quality Action Team that, in 2018, released best practices based on the National Institute of Standards and Technology's Cybersecurity Framework to help towing vessel and barge operators identify and manage cyber risks and detect and respond to cyber-attacks. It is in this spirit of strong partnership that we offer the following recommendations.

The primary principle of the Towing Industry Cyber Risk Management Quality Action Team, and a point that AWO has reiterated since our first comments to the Coast Guard on cybersecurity in 2015,[1] is that towing vessel and barge operators are incredibly diverse in size and organizational complexity. Some have thousands of employees and hundreds of vessels managed with complex information technology (IT) and operational technology (OT) systems, while others employ fewer than two dozen mariners and shoreside staff, operate no more than a handful of vessels, and keep paper records. Between these two extremes are any number of different approaches to the use of cyber-connected systems, and equally important, any number of different arrangements for access to cybersecurity expertise, from in-house IT departments to outsourced IT services. Because of this extensive variability, it has been AWO's longstanding position that when it comes to cybersecurity, one size does not fit all, and it is critical that any cybersecurity guidance or regulations established by the Coast Guard be risk-based and scalable.

A More Risk-Based Approach is Needed for U.S.-Flagged Vessels

The Coast Guard states that through this NPRM, it "proposes to implement a risk-based regulatory, compliance, and assessment regime." However, it is AWO's strong belief that, as applied to the owners and operators of U.S.-flagged vessels subject to 33 CFR Part 104, the proposed Subpart F is not sufficiently risk-based. Regardless of the IT or OT systems used by a vessel, the cybersecurity risks associated with these systems, and the extent to which these risks could result in operational disruption or other harmful consequences, the vessel is subject to the same set of prescriptive requirements with which all other vessels must comply: the vessel must have a designated Cybersecurity Officer (CySO) with specific qualifications and responsibilities; the CySO must develop, implement, and verify a Cybersecurity Plan for the vessel with fixed elements; the CySO must ensure the conduct of drills and exercises on a stipulated schedule; and the owner or operator must comply with specific cybersecurity measures, including strict cybersecurity training requirements for not only vessel personnel but also contractors. This is an onerous regulatory regime to impose on any vessel operator, let alone one with minimal technology use.

This is also a significant regulatory escalation for most U.S.-flagged vessel operators subject to 33 CFR Part 104. The Coast Guard has developed comprehensive cybersecurity requirements and guidance for the owners and operators of U.S. and OCS facilities to address cybersecurity in their facility security assessments and plans through Navigation and Vessel Inspection Circular (NVIC) 01-20, *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*. For U.S.-flagged vessels subject to MTSA, no correspondingly robust requirements or guidance have been forthcoming from the Coast Guard. Instead, the Coast Guard has issued CVC-WI-027(2), *Vessel Cyber Risk Management Work Instruction*, primarily to assist marine inspectors in evaluating the safety management systems of vessels subject to the International Safety Management (ISM) Code for compliance with the International Maritime Organization's cybersecurity requirements, and secondarily to provide guidance on assessing cyber risk management onboard non-ISM Code U.S. vessels. Whereas NVIC 01-20 provides detailed examples of how cybersecurity vulnerabilities may be

[1] The American Waterways Operators. "RE: Guidance on Maritime Cybersecurity Standards (Docket No. USCG-2014-1020)." April 15, 2015.

identified during a facility security assessment and incorporated into a facility security plan, the guidance offered by CVC-WI-027(2) for non-ISM Code U.S. vessels subject to MTSA reads only:

> "A vessel owner must consider cybersecurity vulnerabilities when conducting the vessel's VSA in accordance with 33 CFR 104.305. Cybersecurity vulnerabilities should be addressed per 33 CFR 104.305(d)(2)(v) ['The VSA report must address radio and telecommunication systems, including computer systems and networks'] and 33 CFR 104305(d)(2)(vi) ['The VSA report must address…other areas that may, if damaged or used illicitly, pose a risk to people, property, or operations on board the vessel or within a facility']."

AWO strongly recommends that the Coast Guard develop a new, risk-based approach to cybersecurity requirements for MTSA-regulated vessels, either as part of a separate rulemaking project or in a supplemental notice of proposed rulemaking. We propose an approach that utilizes tiers to apply cybersecurity requirements based on the cybersecurity risk exposure of the vessel. Under this proposal, the vessel's cybersecurity risk exposure would be determined by a Cybersecurity Risk Assessment that differs from the broad, loosely defined Cybersecurity Assessment proposed by the Coast Guard in Subpart F. We recommend a Cybersecurity Risk Assessment that guides vessel operators through a series of questions that evaluate the vessel's connectivity and technology use; regulatory compliance needs; and history of cybersecurity incidents, among other relevant factors. Based on the results of the Cybersecurity Risk Assessment, the vessel would be assigned a tier. The tiers and associated cybersecurity requirements could be:

- Tier I: Minimal Technology Use
  - Conduct a basic cybersecurity risk assessment focusing on critical IT and OT systems annually.
  - Implement basic cyber hygiene practices such as regular software updates, basic user training, and password security.
  - Develop a simple incident response plan that includes steps to respond to cyber incidents and recover operations, using external resources as required.

- Tier II: Moderate Technology Use
  - Tier I requirements, plus:
  - Perform a detailed cybersecurity risk assessment annually.
  - Implement advanced cybersecurity measures, including firewalls, endpoint detection and response, and vulnerability scanning.
  - Conduct regular cybersecurity awareness training for all employees, focusing on phishing, social engineering, and best practices.
  - Hold routine cybersecurity drills.

- Tier III: Extensive Technology Use
  - Tier I and Tier II requirements, plus:
  - Foster a strong cybersecurity culture across the organization, including top-down commitment from leadership and employee engagement.

- Establish processes to evaluate and monitor the cybersecurity practices of vendors and third parties.
- Select and adopt a recognized cybersecurity framework to guide risk management activities.
- Conduct annual penetration testing to validate cybersecurity countermeasures.

AWO acknowledges that our proposed approach is radically different from the approach proposed in the NPRM. However, because it is tailored to the actual risk profile of a vessel, it will ensure that the Coast Guard does not impose infeasible cybersecurity regulatory requirements, with their associated costs and other burdens, that are not commensurate with the vessel's cybersecurity risks. AWO believes that this approach is much more responsible than the NPRM's approach and urges the Coast Guard to change course.

A Cybersecurity Plan Should be Permitted to be Developed and Implemented through an ASP

As proposed, Subpart F makes only one oblique reference to ASP provisions in §101.660, Cybersecurity Compliance Documentation; otherwise, the NPRM does not reference ASPs at all. AWO believes that this is a significant oversight on the part of the Coast Guard. ASPs have been tremendously successful in managing vessel and facility security risks while reducing costs and administrative burdens for both the MTSA-regulated community and the Coast Guard. The AWO ASP not only promotes compliance with 33 CFR part 104 among operators of MTSA-regulated towing vessels and barges, but also ensures the security measures implemented by the operators of these vessels are risk-based, saves these vessel operators the costs of developing thousands of individual vessel security plans, and saves the Coast Guard the costs of reviewing and approving thousands of individual vessel security plans.

AWO urges the Coast Guard to permit a cybersecurity plan to be included in an ASP or as an annex to an ASP. This change would not only enhance the risk-based approach of the proposed regulatory, compliance, and assessment regime for cybersecurity, but also create significant cost savings for vessel and facility operators, as well as the Coast Guard, as compared to the proposed Subpart F, while ensuring the effective management of cybersecurity risks and the protection of the MTS. To accomplish this, AWO strongly recommends that the Coast Guard add to the proposed Subpart F a new §101.670, Alternatives, that is modeled on 33 CFR §101.120 and aligned with the requirements for Cybersecurity Plans in the proposed §101.630, to provide that owners and operators of vessels and facilities required to have Cybersecurity Plans under Subpart F may meet the requirements of an ASP that has been reviewed and approved by the Commandant as meeting the requirements of Subpart F, as applicable.

Section 101.605—Applicability

Barge Fleeting Facilities Should be Exempt

The affected population of facilities subject to 33 CFR Part 105 includes barge fleeting facilities that receive barges carrying, in bulk, cargoes regulated by 46 CFR subchapter I, inspected under 46 CFR, subchapters D or O, or certain dangerous cargoes (CDC). As most barge fleeting facilities service CDC barges occasionally, the vast majority of barge fleeting

facility operators would be required to comply with the proposed Subpart F. The application of Subpart F to these facilities is neither practical nor justified.

Barge fleeting facilities are very different from large marine terminals, refineries, and chemical plants in terms of infrastructure, activity, personnel, the use of cyber-connected systems, and associated security risks. Many of these facilities are located in rural areas isolated from major population centers. Only a small percentage of fleeting facilities have shoreside access; the vast majority are accessible only via a towing vessel that monitors the security of the fleeting area and provides authorized individuals with access to and from the moored barges. The barges moored within the fleeting area are unmanned. Unlike fixed maritime facilities, most barge fleeting facilities have no permanent infrastructure, including electricity and internet access.

Given that the IT and OT systems used by operators of barge fleeting facilities are very limited, and that the cybersecurity risks to which these facilities are exposed are extremely minimal, AWO does not believe that the decision to require these facilities to comply with the proposed Subpart F is risk-based. Requiring each barge fleeting facility to create a Cybersecurity Plan, implement cybersecurity measures, and designate an individual with the responsibilities and qualifications of a Cybersecurity Officer will impose significant costs on barge fleeting facility operators without accruing commensurate benefits to the security of the MTS. We urge the Coast Guard to exempt barge fleeting facilities from the proposed Subpart F.

The Exemption of Foreign-Flagged Vessels Creates an Unlevel Playing Field

Currently, both U.S-flagged and foreign-flagged vessels operating internationally are subject to the International Ship and Port Facility Security (ISPS) Code, as well as the IMO's *Guidelines on Cyber Risk Management* and Maritime Security Committee Resolution 428(98), *Maritime Cyber Risk Management in Safety Management Systems*, which requires vessel operators to "take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code." Further, to ensure that foreign-flagged vessels in U.S. waters maintain the security of the MTS, the Coast Guard applies certain requirements of 33 CFR Part 104 that are not comprised in the International Ship Security Certificate to foreign-flagged vessels, creating equivalency with U.S.-flagged vessels.

However, the Coast Guard is now exempting foreign-flagged vessels from the proposed Subpart F. In the preamble of the NPRM, the Coast Guard states that "based on IMO guidelines and recommendations, an SMS approved under the ISM Code should address foreign-flagged vessel cybersecurity," and the process described in CVC-WI-027(2) "would continue to be the Coast Gurd's primary means of ensuring cybersecurity readiness on foreign-flagged vessels." This standard is substantially less costly and burdensome than the standard that would be imposed on U.S.-flagged vessels by Subpart F, putting U.S.-flagged vessels at a significant competitive disadvantage—despite the fact that the risks posed to the MTS by a cybersecurity incident on a U.S.-flagged vessel are not appreciably different from a cybersecurity incident on a foreign-flagged vessel in U.S. waters. AWO encourages the Coast

Guard to level the playing field by ensuring that the cybersecurity requirements applicable to U.S.-flagged vessels are also applied to foreign-flagged vessels U.S. waters.

Section 101.615—Definitions

Cyber Incidents Should be Reported to the National Response Center

The Coast Guard is seeking comments on two alternative processes for reporting cyber incidents: a requirement to report to the National Response Center (NRC), which is consistent with established practice, or a requirement to report to the Cyber and Infrastructure Security Agency (CISA), which "could allow more efficient use of [the Department of Homeland Security's] cybersecurity resources and may advance the cybersecurity vision laid out by Congress in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)."[2] AWO urges the Coast Guard to continue to require that reportable cyber incidents are reported to the NRC for two reasons.

First, we support the Coast Guard as the designated federal agency for reporting cyber incidents involving MTSA-regulated vessels and facilities because the Coast Guard has longstanding authority over, as well as demonstrated expertise and a vested interest in, securing the MTS. The Coast Guard is best placed to assess the potential or actual threats that a cyber incident poses to vessel and facility operations and the broader MTS and has proven itself as a trusted partner in handling all reports of cyber incidents as Sensitive Security Information (SSI).

Second, consistent with 33 CFR §101.305, vessel operators and crewmembers are already accustomed to reporting suspicious activities (SA), activities that may result in a transportation security incident (TSI), and breaches of security (BOS) to the NRC. The NRC is also the designated federal point of contact for reporting discharges of oil, hazardous substances, or marine pollutants per 33 CFR §151.15. Establishing a single telephone channel for incident reporting, regardless of the type of incident, promotes compliance with reporting requirements and the timeliness of reporting by substantially reducing the risk that a reporter will be confused or have hesitation about proper reporting requirements—especially in the acute stress that an incident may precipitate. It also simplifies company procedures and employee training, and therefore reduces costs and other burdens for vessel operators and crewmembers. Conversely, establishing a separate email or telephone channel for reporting cyber incidents to CISA increases the likelihood that a reporter will mistakenly report to the wrong entity or delay reporting to confirm reporting requirements, and imposes costs and other burdens by obliging vessel operators to develop new procedures and training. AWO strongly believes that the prerequisite for efficient incident response is efficient incident reporting, which is advanced by clear and consistent reporting requirements.

AWO notes that member companies have experienced wait times when calling the NRC to submit incident reports. We encourage the Coast Guard to ensure that the NRC is adequately staffed to meet increases in demand, minimize wait times, and provide effective, responsive service to support the federal government and the regulated community in incident response.

[2] 89 Federal Register 13410.

Duplicative Reporting Obligations Created by E.O. 14116 Should be Streamlined

On February 21, one day prior to the publication of the NPRM in the Federal Register, President Biden issued an Executive Order 14116, *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States.* Among other measures, E.O. 14116 amends 33 CFR §6.16-1 to read:

> "Evidence of sabotage, subversive activity, or an actual or threatened cyber incident involving or endangering any vessel, harbor, port, or waterfront facility, including any data, information, network, program, system, or other digital infrastructure thereon or therein, shall be reported immediately to the Federal Bureau of Investigation, [CISA] (for any cyber incident), and the Captain of the Port, or to their respective representatives."

E.O. 14116 also establishes the definition of "cyber incident" at 33 CFR §6.01-8 as equivalent to the definition of "incident" at 44 U.S.C. 3552(b)(2), which reads:

> "The term "incident" means an occurrence that—(A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or, (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

The Coast Guard concurrently published NVIC 02-24, *Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents*, to provide guidance on these new reporting requirements. As noted in section 3.b of the NVIC, "The broad applicability of 33 CFR Part 6 and the new definition of a cyber incident created an overlap with existing MTSA reporting requirements," which the NVIC is intended to clarify. Helpfully, section 1.e.3 of Enclosure (1) to the NVIC clarifies that cyber incidents reported to the NRC or Captain of the Port (COTP) as a BOS, SA, or TSI do not need to be reported to the FBI or CISA. However, any other cyber incidents that meet the broad definition of 33 CFR §6.01-8 must be reported to the FBI, CISA, and COTP, and further, "a notification to the NRC is recommended," although if it is confirmed that the NRC report will be sent to the COTP, the submission of a separate report to the COTP is not necessary. In short, at least three separate cyber incident reports must be submitted to three separate federal agencies. These reporting requirements not only have the potential to be confusing for reporters but also are duplicative and burdensome for the regulated community. Section 5.c of the NVIC states, "The purpose of this requirement is to provide the FBI, CISA, and Coast Guard the opportunity to understand and respond to potential or actual threats to the MTS upon receipt of a report, and determine appropriate action." AWO argues that the burden of information-sharing and coordination among relevant federal agencies should fall on those agencies, not on the regulated community. We urge the Coast Guard to establish a process for the NRC to share cyber incident reports that meet the 33 CFR §6.01-8 definition with the FBI and CISA as well as the COTP so that reporters can meet the reporting requirements of 33 CFR §6.16-1 with a single report to the NRC.

The Forthcoming CIRCIA Rule Should Not Create Duplicative Reporting Obligations

On April 4, CISA published a proposed rule to implement CIRCIA's mandate to promulgate regulations requiring covered entities to report cyber incidents and ransom payments made in response to a ransomware attack. CISA proposes to include MTSA-regulated vessel and facility operators in its definition of a covered entity. AWO appreciates the Coast Guard's explicit statement in the NPRM that, "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."[3] This is aligned with CISA's proposed regulation, which states, "A covered entity that reports a covered cyber incident, ransom payment, or information that must be submitted to CISA in a supplemental report to another Federal agency pursuant to the terms of a CIRCIA Agreement will satisfy the covered entity's reporting requirements under §226.3."[4] We assume, based on the NPRM and its reference to 6 U.S.C. §681b(a)(5)(B)[5], that the Coast Guard has entered or plans to enter into a CIRCIA Agreement with CISA, and we welcome this step to reduce reporting burdens on the MTSA-regulated community.

The Coast Guard writes in the NPRM that it is inviting comments "on whether we should expressly require reporting of ransom payments in connection with ransomware attacks."[6] We support the Coast Guard's establishment of such a requirement to reinforce a single process for incident reporting for MTSA-regulated vessel and facility operators and ensure these entities are not required to report such incidents separately to CISA. However, CISA's proposed regulations are open for public comment until July 3, and it is possible that due to the agency's adjudication of the public comments it receives, the requirements for reporting ransom payments will undergo significant changes. Any Coast Guard requirement to report ransom payments should be harmonized with, and no more stringent than, CISA's final rule to implement CIRCIA.

The Definition of Reportable Cyber Incident Should Be Refined

The Coast Guard writes in the NPRM that it "welcomes comments on whether we should define and use the term *Reportable cyber incident*," which if adopted "would replace *cyber incident* in proposed §§101.620(b)(7) and 101.650(g)(1)."[7] AWO supports the definition of reportable cyber incident to "establish a threshold between the cyber incidents that must be reported and the ones that do not."[8] AWO believes that the definition of cyber incident in the proposed §101.615 is both too broad and too narrowly and inappropriately focused on IT to be a reasonable basis for reporting. However, AWO has concerns with the proposed definition of reportable cyber incident and its alignment, or lack thereof, with other definitions for reportable cyber incidents in regulation and policy.

---

[3] 89 Federal Register 13410.
[4] 89 Federal Register 23769.
[5] 89 Federal Register 13410 (footnote 37).
[6] Ibid.
[7] 89 Federal Register 13409.
[8] Ibid.

The proposed definition of reportable cyber incident presented in the NPRM is:

> "an incident that leads to, or, if still under investigation, could reasonably lead to any of the following: (1) Substantial loss of confidentiality, integrity, or availability of a covered information system, network, or OT system; (2) Disruption or significant adverse impact on the reporting entity's ability to engage in business operations or deliver goods or services, including those that have a 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."[9]

This proposed definition is generally aligned with the guidance provided by the Coast Guard in section 1.a of Enclosure (1) of NVIC 02-24 to clarify what is reportable under the cyber incident definition in 33 CFR §6.01-8. However, that guidance includes important stipulations, such as "routine spam, phishing attempts, and other nuisance events that do not breach a system's defenses may not need to be reported as cyber incidents," and "accidental violation of acceptable use policies, such as plugging in an unauthorized USB device, is not considered a reportable cyber incident." That guidance also states, "The Coast Guard recognizes that the cyber domain includes countless malicious but low-level events that are normally addressed via standard anti-virus programs and similar protocols. MTS stakeholders should report events that are out of the ordinary in terms of sophistication, volume, or other factors which, from the operator's perspective, raise suspicions and may result in a TSI."

AWO agrees that the threshold for cyber incidents that must be reported and the ones that do not should be the potential that the cyber incident could result in a TSI. It is an unfortunate reality of the current cyber threat environment that all businesses, regardless of sector, experience regular—even frequent—"nuisance" or "low-level" events, and that preventing, mitigating, and resolving these events is a necessary business function. A definition of reportable cyber incident that did not exclude such events would result in an incalculable volume of reports that would impose unmanageable burdens on both MTSA-regulated vessel and facility operators and the Coast Guard and would have negligible benefits in safeguarding the MTS. Further, through MTSA, Congress gave the Coast Guard the authority to "identify, assess, and prevent TSIs in the MTS,"[10] and through the NPRM, the Coast Guard proposes regulations to "help detect, respond to, and recover from cybersecurity risks that may cause [TSIs]."[11] Therefore, events that do not have the potential to result in a TSI not only have little to no value as reportable cyber incidents but also are outside the scope of this rulemaking.

With this in mind, AWO recommends the following changes to the proposed definition of reportable cyber incident:

---

[9] Ibid.
[10] 89 Federal Register 13406.
[11] 89 Federal Register 13405.

- Element (1) should be amended to read, "Substantial loss of confidentiality, integrity, or availability of a ~~covered information system, network, or OT system~~ critical information technology or operational technology system." Per the definition of *Critical Information Technology (IT) or Operational Technology (OT) systems* in the proposed §101.615, these are systems "that, if compromised or exploited, could result in a transportation security incident, as determined by the Cybersecurity Officer (CySO) in the Cybersecurity Plan." AWO believes that this amendment will better assist vessel and facility operators in determining reportability and better ensure that reported cyber incidents are linked to the potential to cause a TSI, as opposed to a routine and manageable nuisance or low-level event.

- Element (2) should be amended to read, "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." This amendment will better align element (3) with the associated element of CISA's proposed definition of *Substantial cyber incident*[12] and will also eliminate an ambiguous term that is not meaningfully different from the term "disruption."

- Element (3) should be amended to read, "~~Disclosure or~~ Unauthorized access ~~directly or indirectly of non-public personal information of a significant number of individuals~~ to an information system or network, or any nonpublic information contained therein, that is facilitated through or caused by a: (i) Compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (ii) Supply chain compromise." AWO believes that, as proposed, element (3) does not link unauthorized access of nonpublic information to a potential TSI, and further, could conflict with other federal and state regulations and contractual agreements requiring vessel and facility operators, as business owners, to protect nonpublic information. We are concerned that this creates an obligation to report cyber incidents that are not associated with threats to vessel or facility operations or the broader MTS, could lead to non-compliance with other regulatory or contractual obligations, and may compromise confidential business information. We also note that the phrase "a significant number of individuals" is vague and very subjective. This amendment will align element (3) with the associated element of CISA's proposed *Substantial cyber incident* definition.[13] We believe that this will better ensure the substantial similarity of the Coast Guard and CISA's reporting requirements, and moreover, that this is a more reasonable requirement because, as CISA puts it, compromises of third-party service providers or supply chains "uniquely have the ability to cause significant or substantial nation-level impacts, even if the impacts at many of the individual covered entities are relatively minor."[14]

- Element (4) should be deleted because it uses terms that are vague ("potential operational disruption") or undefined ("critical infrastructure systems and assets")

[12] 89 Federal Register 23767.
[13] Ibid.
[14] 89 Federal Register 23664.

within the proposed Subpart F; it is inconsistent with CISA's proposed definition of substantial cyber incident, and more importantly, it is redundant to element (5). It is difficult to envision an incident that would lead to potential operational disruption to critical infrastructure systems or assets that does not meet the definition of a potential TSI.

Section 101.625—Cybersecurity Officer

In proposed §101.625, the Coast Guard has created a requirement for a Cybersecurity Officer (CySO), a new organizational position with an extensive list of responsibilities and required qualifications. This requirement has the potential to impose significant costs and other burdens on the largest and most well-resourced vessel operators, let alone small vessel operators with limited resources. AWO urges the Coast Guard to reconsider the role of the CySO as applied to MTSA-regulated towing vessel and barge operators and offers the following comments and recommendations.

The CySo Should Not Be Required to Be a Cybersecurity Subject Matter Expert

In its cost analysis of the NPRM, and specifically, its analysis of cybersecurity plan costs, the Coast Guard states, "For the purpose of this analysis, we assume that an existing person in a facility, OCS facility, or U.S.-flagged vessel company or organization would assume the duties and responsibilities of a CySO, and that owners and operators would not have to hire an individual to fill this position."[15] This assumption is incorrect. As currently conceived, the CySO position requires too much specialized knowledge and experience and too much time to be added to an existing security officer or other employee's role. Small member companies that outsource IT services have advised AWO they have no employees that can fulfill the CySO role. Mid-sized member companies may employ an IT manager but use a managed service provider as a cybersecurity operations center because the IT manager is fully occupied with standard IT issues. Even the largest companies in the tugboat, towboat, and barge industry, with in-house IT departments, tell AWO that they would have to hire an individual to fill the CySO position. Therefore, an accurate cost analysis should have included, at a minimum, the mean annual wage of one information security analyst per vessel operator, or 1,775 × $119,860[16], for a total cost of $212,751,500 on an annual basis.

The Coast Guard's proposed qualifications for CySOs make it clear that this role demands more expertise than an existing security officer or other employee can reasonably be expected to possess. §101.625(e) requires the CySO to "have general knowledge" on the listed topics "through training or equivalent job experience." Since vessel operators are not currently subject to extensive cybersecurity requirements, few companies employ existing persons with significant cybersecurity training or job experience—especially because individuals with this training or job experience are in high demand and command high salaries. Most existing company or vessel security officers or other employees would therefore be obliged to undergo training in order to qualify as a CySO. Further, given the highly dynamic and fast-evolving

[15] 89 Federal Register 13423.
[16] AWO obtained this wage from the same BLS website at https://www.bls.gov/oes/2022/may/oes151212.htm used by the Coast Guard in its analysis, as referenced at 89 Federal Register 13423.

nature of the cyber threat environment, many of the topics listed in §101.625(e)—including, but certainly not limited to, general cybersecurity guidance and best practices, relevant laws and regulations pertaining to cybersecurity, and current cybersecurity threat patterns and Known Exploited Vulnerabilities (KEVs)—will require ongoing training or professional development.

Due to the limited number of critical IT or OT systems used by towing vessels and barges and the segmentation of vessel networks, AWO does not believe it is necessary for the CySO for such vessels to be a subject matter expert in cybersecurity. We argue that the duties associated with the implementation of a Cybersecurity Plan can be assigned to an existing security officer or other employee that does not have specialized cybersecurity training or job experience. In our view, the CySO's role should be similar to the CSO's role, with primary responsibilities for ensuring the requirements of the Cybersecurity Plan are met, and with the ability to secure access to cybersecurity expertise, whether internal or external, as needed. In AWO's assessment, the number of proposed CySO responsibilities that could necessitate cybersecurity expertise is limited, pertaining to the conduct of the Cybersecurity Assessment, the development of the Cybersecurity Plan, taking corrective actions for problems identified by exercises, audits, or inspections, and the identification and mitigation of KEVs in critical IT and OT systems. Many CSOs utilize external service providers to conduct a Vessel Security Assessment and develop and update a Vessel Security Plan, or participate in an ASP. Likewise, if needed, the CySO can utilize external service providers to conduct the Cybersecurity Assessment and develop and update the Cybersecurity Plan, or implement an ASP with a Cybersecurity Plan annex. Responsibilities for corrective actions and the identification and mitigation of KEVs can be assigned by the CySO to internal IT managers or external IT or cybersecurity service providers.

Therefore, AWO recommends that §101.625(e)—at least as it applies to MTSA-regulated towing vessels and barge operators—be amended to read:

> "*Qualifications.* The CySO must have general knowledge~~, through training or equivalent job experience,~~ in the following:
> (1) General vessel, facility, or OCS facility operations and conditions;
> ~~(2) General cybersecurity guidance and best practices;~~
> (3) The vessel, facility, or OCS facility's Cyber Incident Response Plan;
> (4) The vessel, facility, or OCS facility's Cybersecurity Plan;
> ~~(5) Cybersecurity equipment and systems;~~
> (6) Methods of conducting ~~cybersecurity~~ audits, inspections, control, and monitoring techniques;
> ~~(7) Relevant laws and regulations pertaining to cybersecurity;~~
> (8) Instruction techniques for ~~cybersecurity~~ training and education;
> (9) Handling of Sensitive Security Information and security related communications; and
> ~~(10) Current cybersecurity threat patterns and KEVs;~~
> ~~(11) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security; and~~
> (12) Conducting and assessing ~~cybersecurity~~ drills and exercises."

The Company Security Officer Should Be Permitted to Serve as the CySO

The Coast Guard proposes in §101.625(a) to permit the CySO to "perform other duties within the owner's or operator's organization (vessel or facility), provided the person is able to perform the duties and responsibilities required of the CySO by this part," and in §101.625(b) to permit the same person to "serve as the CySO for more than one vessel, facility, or OCS facility." Elsewhere in the preamble, the Coast Guard states, "For facilities and OCS facilities, this person may be the Facility Security Officer. For vessels, this person may be the Vessel Security Officer."[17] The Coast Guard should clarify that this person may also be the CSO. Provided that the CSO is able to perform the CySO's duties and responsibilities, there should be no limitation on their ability to do so.

Other Recommendations

- §101.625(d)(15) requires the CySO to "[e]nsure identification and mitigation of all KEVs in critical IT or OT systems, without delay." AWO does not believe that this requirement is reasonable and recommends that the Coast Guard amend the provision to read, "Ensure the timely identification and mitigation of all applicable KEVs that pose an imminent threat to critical IT or OT systems~~, without delay~~."

Section 101.635—Drills and Exercises

Drills Should Be Less Frequent and at the Organizational Level, not the Vessel Level

The Coast Guard proposes in §101.635(b) to require the conduct of at least one cybersecurity drill every 3 months. Although it is not explicit, AWO assumes the Coast Guard means to apply this requirement to each vessel. This is excessive given the limited number of cybersecurity risks that may be faced by a vessel. It is also burdensome for vessel operators and crewmembers, who are already subject to extensive requirements for safety, security, and other drills, and who may have little to no role in vessel cybersecurity. Further, on towing vessels, drills are generally supervised by the master of the vessel, who is unlikely to have cybersecurity expertise and would therefore require training to manage this added responsibility. AWO recommends that the Coast Guard amend this requirement to require the conduct of drills at the organizational level instead of the vessel level and to tie the frequency of the drills to the risk profile of the operator—at least one drill every year for Tier 1 and Tier 2 operators and at least one drill every six months for Tier 3 operators.

Section 101.650—Cybersecurity Measures

Proposed Account Security Measures Should Be Revised for Vessels

The Coast Guard's proposed §101.650(a)(4) states, "Multifactor authentication must be implemented on password-protected IT and remotely accessible OT systems." This requirement is not feasible for vessels for two reasons. First, vessels may have limited or

[17] 89 Federal Register 13422.

intermittent connectivity to internet, phone, or SMS networks, so implementing multifactor authentication may result in users being unable to access secondary credentials when they need to use a password-protected system. Second, vessel crewmembers frequently rotate on and off vessels and from one vessel to another, making it extremely challenging to maintain multifactor authentication credentials for individual users; in fact, due to high crewmember turnover, many vessels have established role-based as opposed to user-based accounts for onboard IT and OT systems, which are not compatible with multifactor authentication. Because vessel networks are segmented from each other and from shoreside networks, AWO does not believe that multifactor authentication is necessary to mitigate cybersecurity risks, and therefore, we recommend that the Coast Guard exempt vessels from this provision.

Proposed Data Security Measures Should Be Clarified

The Coast Guard's proposed §101.650(c) states, "Data logs must be securely captured, stored, and protected so that they are accessible only by privileged users," and "all data, both in transit and at rest, must be encrypted using a suitably strong algorithm." The term "data logs" is undefined, so it is unclear what the Coast Guard is proposing to require, and whether algorithm encryption is appropriate. AWO asks the Coast Guard to clarify this requirement.

Cybersecurity Training for Personnel Should Not Include Contractors

The Coast Guard's proposed §101.650(d) states, "All personnel with access to the IT or OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must have cybersecurity training" in prescribed topics, and, "Key personnel with access to the IT or remotely accessible OT systems, including contractors, whether part-time, full-time, temporary, or permanent, must also have cybersecurity training" in additional topics. AWO does not believe that it is reasonable to include contractors in the cybersecurity training requirements. In the real world, a contractor may visit a vessel once and never again, or may be dispatched in the middle of the night to fix an urgent problem; in these and many other circumstances, requiring a contractor to undergo cybersecurity training is excessive and has the potential to impede vessel operation. AWO urges the Coast Guard to eliminate the requirement for contractors to have cybersecurity training.

The Timeline for Implementing Cybersecurity Training for Personnel Should be Extended

The Coast Guard's proposed §101.650(d)(3) states that all personnel and all key personnel must complete the specified training by the date 180 days after the effective date of the final rule. AWO does not believe that six months is a sufficient amount of time for a vessel operator to develop a Cybersecurity Plan and develop and implement cybersecurity training on that Cybersecurity Plan. AWO recommends that the Coast Guard extend the deadline for completion of cybersecurity training to the date 365 days after the effective date of the final rule.

Cost Analysis

The Coast Guard's cost analysis significantly underestimates the costs to vessel operators of implementing the proposed Subpart F. For example, in its analysis of the costs of cybersecurity drills, the Coast Guard states that "the only new cost associated with the proposed cybersecurity drills is the development of cybersecurity components to add to existing drills," and estimates that "it would take a CySO 0.5 hours (30 minutes) to develop new cybersecurity components to add to existing drills."[18] This reflects a poor understanding of the process of administering drills, and does not take into account the costs of training vessel crewmembers to supervise drills, documenting the conduct of drills, identifying lessons learned, and disseminating information to employees. AWO encourages the Coast Guard to consult vessel operators, and not just Coast Guard or CISA SMEs, to develop a more accurate understanding of the substantial time burdens and costs of its proposed requirements on vessel operators.

AWO appreciates the opportunity to provide comments on the Coast Guard's proposed regulations for cybersecurity in the MTS and would be pleased to answer any questions or provide any additional information.

Sincerely,

Jennifer Carpenter

Jennifer Carpenter
President & CEO

[18] 89 Federal Register 13428.