The American Waterways Operators

801 North Quincy Street
Suite 500
Arlington, VA 22203

PHONE: 703.841.9300
EMAIL: cstewart@americanwaterways.com

Caitlyn E. Stewart
Vice President – Regulatory Affairs

March 18, 2025

Rear Admiral 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 Maritime Transportation System Final Rule and Request for Comments (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 final rule to establish minimum cybersecurity requirements for U.S.-flagged vessels and facilities subject to the Maritime Transportation Security Act of 2002 (MTSA).

For nearly 25 years, AWO has worked in partnership with the Coast Guard to ensure the security of the marine transportation system. We take seriously our role as operators and guardians of critical infrastructure in the maritime domain, and we recognize the threat of cyber-attacks to disrupt the safety, security and continuity of maritime commerce and the U.S. supply chain. However, as we stated in our comments of May 22, 2024, on the proposed rule, we strongly believe that the diversity in size, organizational complexity, and use of information technology (IT) and operational technology (OT) among companies in the tugboat, towboat and barge industry demands cybersecurity regulations that are risk-based and scalable.

We remain concerned that the final rule imposes onerous requirements that are not sufficiently risk-based and are a significant regulatory escalation for most affected U.S.-flagged vessel operators. Further, we do not believe that the Coast Guard adequately addressed the comments from U.S.-flagged vessel operators urging a more risk-based approach. As a result, we urge the Coast Guard to: 1) delay the implementation of the final rule for U.S.-flagged vessel operators;

and 2) reopen the comment period for an additional 60 days to solicit further public comments and conduct a more comprehensive review of alternative approaches to the final rule.

**Delay Implementation for U.S.-Flagged Vessel Operators**

The final rule is broad, technically complex, and affects a wide range of vessel types, operations, personnel and equipment. Vessel operators need more time to understand and develop compliance strategies for these requirements. Prior to the finalization of this rule, and in contrast with the Coast Guard's approach to U.S. facilities[1], there had been no prescriptive or detailed cybersecurity requirements or guidance applied to U.S.-flagged vessels[2], making compliance with these requirements a much more difficult undertaking. Further, most of AWO's members do not have IT personnel with specialized knowledge and experience in cybersecurity or with the ability to take on a compliance project of this magnitude in addition to other duties. And importantly, the final rule imposes significant and unplanned costs that will be hard for vessel operators to absorb within the timelines. Under these circumstances, it will be extremely challenging for a vessel operator to meet the current compliance deadlines.

The final rule requires training to be provided to vessel personnel and contractors with access to IT and OT systems within six months of the effective date of the rule. In order to comply, a vessel operator must develop a new cybersecurity training program, identify the personnel and contractors required to be trained, and provide the required training by January 16, 2026 – an aggressive timeline. In our previous comments, AWO had recommended that the Coast Guard extend the deadline for completion of cybersecurity training to 12 months after the effective date of the rule, and we reiterate that recommendation here.

The final rule also requires the Cybersecurity Assessment to be conducted and the Cybersecurity Plan to be submitted to the Coast Guard for approval within 24 months of the effective date of the rule. It is not realistic for vessel operators to conduct a Cybersecurity Assessment and develop a Cybersecurity Plan by July 16, 2027, and it is AWO's strong recommendation that these requirements be delayed for a period of five years.

Adhering to the current compliance deadline for Cybersecurity Assessments and Cybersecurity Plans will strain the resources of both the regulated community and the Coast Guard. If all affected entities are required to conduct Cybersecurity Assessments and develop Cybersecurity Plans within a two-year period, we anticipate an acute increase in the need for maritime cybersecurity expertise, which is already in short supply and will exacerbate both the high demand and high costs for individuals with this skill set. In addition, the likely outcome is that Cybersecurity Plans for most affected entities will be submitted to the Coast Guard at or near the deadline, placing significant burdens on the agency personnel responsible for reviewing these plans both initially and at five-year intervals into the future. This is aggravated by the fact that, as the agency admits in its response to comments, "The Coast Guard has not yet identified where ownership of initial and subsequent review of Cybersecurity Plans will reside, but will determine that upon assessing the process that optimizes resources and expertise."

---

[1] See Navigation and Vessel Inspection Circular (NVIC) 01-20, *Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities.*

[2] See CVC-WI-027(2), *Vessel Cyber Risk Management Work Instruction.*

Given the anticipated volume of submissions, this raises concerns about the Coast Guard's ability to conduct reviews in a timely, efficient and effective manner[3].

Delaying implementation for these requirements by a period of five years for U.S.-flagged vessel operators will allow for Cybersecurity Assessments to be conducted and Cybersecurity Plans to be developed on a much more reasonable timeline. It will provide time for operators to phase in the requirements for compliance incrementally, secure their personnel the necessary training or job experience or procure contracted resources, and defray costs, and it will avoid the pitfalls of cost shocks. It will also increase the likelihood that submissions of Cybersecurity Plans to the Coast Guard are staggered over time and allow the agency sufficient time to establish a process for the review of Cybersecurity Plans that is supported by the necessary capacity. If a vessel operator would like to include their Cybersecurity Plan in their Vessel Security Plan (VSP), or as an annex to their VSP, they will be able to do so during their next VSP reapproval period. The Coast Guard will have ample time to answer questions that arise during implementation or develop further guidance if needed to facilitate compliance.

The Coast Guard may be concerned that during a five-year implementation delay, cybersecurity risks on U.S.-flagged vessels will not be adequately mitigated. However, vessel cybersecurity vulnerabilities will continue to be identified and addressed through VSPs and Alternative Security Programs (ASPs), and the Coast Guard will continue to be able to exercise oversight through MTSA verification inspections and other vessel inspection activities. To date, these measures have effectively mitigated vessel cybersecurity risks that may cause transportation security incidents (TSI) – as demonstrated by the fact that there has been no TSI caused by the exploitation of a vessel cybersecurity vulnerability.

**Reopen the Comment Period for an Additional 60 Days**

In an effort to meet a deadline for publication set by the previous administration, the Coast Guard's process for reviewing and responding to comments was truncated. We are concerned that comments from U.S.-flagged vessel operators concerning the significant burdens imposed by the rule and the urgent need for a more risk-based approach were not given due consideration. We appreciate that the Coast Guard has recognized there is a role for ASPs as well as waivers and equivalents to facilitate the compliance process and descope the requirements based on risk. However, this is an acknowledgement that certain cybersecurity measures required by the final rule may not be applicable to all affected entities, and these mechanisms place the onus for reducing regulatory burdens on the regulated community. As written, the final rule requires a harbor tug with a non-networked computer and an AIS to meet the same requirements as an international cargo or cruise ship terminal with dozens of sophisticated and interconnected cyber systems. We believe that in the interests of responsible regulation, the Coast Guard should reopen the comment period to solicit additional feedback

[3] Moreover, if a vessel operator wishes to include the Cybersecurity Plan in their Vessel Security Plan (VSP), or as an annex to their VSP, it is not clear how their VSP validity period and reapproval timeline will be impacted. If the entire VSP must be reviewed concurrently with the Cybersecurity Plan, this raises the specter of even more dire consequences.

from the public, conduct a more comprehensive and complete review of the input it receives, and tailor the applicability of requirements according to risk.

Thank you again for the opportunity to comment. AWO would be pleased to provide additional comments or further information as you see fit.

Sincerely,

Caitlyn Stewart
Vice President – Regulatory Affairs