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

June 28, 2024

Ms. Jennie M. Easterly
Director
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, VA 20598

Re: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (CISA-2022-0010)

Dear Director Easterly:

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 Cybersecurity and Infrastructure Security Agency's (CISA) Notice of Proposed Rulemaking (NPRM) to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

AWO has long been committed to working in partnership with federal agencies—and in particular, our foremost regulator, the U.S. Coast Guard—to ensure the security of the marine transportation system. In 2018, recognizing the potential of cyber-attacks to disrupt the continuity of maritime commerce, a Quality Action Team chartered by the Coast Guard-AWO Safety Partnership 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. The primary principle of the Quality Action Team, and a point that AWO has reiterated to the Coast Guard as we have worked together to enhance the cybersecurity of the marine transportation system (MTS), 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 just a few vessels, and keep paper records. Between these two extremes are many different approaches to the use of cyber-connected systems. 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 cybersecurity regulations be risk-based and scalable. In the spirit of partnership, and with this perspective in mind, we offer the following recommendations to CISA on its proposed rule.

Cyber Incident Reporting Requirements

Current cyber incident reporting requirements for the maritime industry are confusing and onerous.

On February 21, President Biden issued Executive Order 14116, *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States*. E.O. 14116 amends 33 CFR §6.16-1 to mandate immediate reporting of "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," to the Federal Bureau of Investigation, CISA, and the cognizant Coast Guard Captain of the Port. It also establishes the definition of "cyber incident" at 33 CFR §6.16-8 as equivalent to the definition of "incident" at 44 U.S.C. 3552(b)(2), which reads: "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 E.O. 14116 definition of cyber incident is inconsistent with CISA's proposed definition of covered cyber incident at §226.1. Further, E.O. 14116 necessitates at least three separate cyber incident reports to three different federal agencies. These conflicting and duplicative regulatory requirements will be confusing and burdensome for the regulated community.

The burden of information-sharing and coordination among federal agencies in the event of a cyber incident should fall on those agencies, not on the regulated community. We appreciate that CISA has recognized the need to reduce reporting burdens on the regulated community by proposing at §226.4 an exemption to its reporting requirements for covered entities that report substantially similar information in a substantially similar timeframe to another federal agency pursuant to an existing law, regulation, or contract when a CIRCIA Agreement is in place between CISA and the other federal agency. As discussed below, we strongly support this approach. We also note that CIRCIA itself, at 6 USC 681g(a)(1), requires any federal agency that receives a report from an entity of a cyber incident, including a ransomware attack, to provide the report to CISA within 24 hours. We believe that this fulfills the purpose of E.O. 14116 to, as the Coast Guard states in implementing policy, "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 actions."[1] Therefore, we encourage CISA and the Coast Guard to work together to ensure that CISA's final rule supersedes the cyber incident definition and reporting requirements of E.O. 14116.

The National Response Center should be the maritime industry's reporting hub for cyber incidents.

[1] U.S. Coast Guard Navigation and Vessel Inspection Circular 02-24, *Reporting Breaches of Security, Suspicious Activity, Transportation Security Incidents, and Cyber Incidents*. Section 5.b., p. 2.

As previously stated, the Coast Guard is the maritime industry's primary federal regulator, and since 2016, that agency has required U.S. vessel and facility operators to report suspicious activities (SA), activities that may result in a transportation security incident (TSI), and breaches of security (BOS)—including cyber incidents—to the National Response Center (NRC) under regulations implementing the Maritime Transportation Security Act (MTSA) at 33 CFR §101.305. On February 22, the Coast Guard published an NPRM, *Cybersecurity in the Maritime Transportation System* (USCG-2022-0802), which sought public comment on two alternative processes for U.S. vessel and facility operators to report cyber incidents: a requirement to report to the NRC, which is consistent with established practice, or a requirement to report to 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" CIRCIA.[2] In our comment letter, AWO urged the Coast Guard to continue to require that cyber incidents be 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, we support the NRC as the cyber incident reporting hub for the maritime industry because vessel operators and crewmembers are already accustomed to reporting cyber incidents 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 all types of maritime incident reports promotes compliance with reporting requirements and supports prompt reporting by substantially reducing the risk that a reporter will be confused or have hesitation about proper reporting procedures, which is crucial during the acute stress that an incident may precipitate. This approach also streamlines organizational procedures and training, thereby reducing costs and other burdens for vessel operators and crewmembers. On the other hand, creating a separate electronic 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 verify the correct procedure, in addition to incurring extra costs and other burdens by obliging organizations to develop new protocols and training. Effective incident response begins with efficient incident reporting, which is best achieved through clear and consistent reporting requirements. Reinforcing the NRC's position as the nexus of maritime incident reporting is the most reasonable and effectual way to achieve this goal.

[2] 89 Federal Register 13410.

CISA has proposed to include MTSA-regulated vessel and facility operators in its definition of a covered entity at §226.2. In its NPRM, the Coast Guard stated 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] We assume, based on this statement and its reference to 6 U.S.C. §681b(a)(5)(B)[4], 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 and permit vessel and facility operators to continue to report cyber incidents to the NRC.

For this reason, AWO recommended that the Coast Guard make changes to its proposed definition of reportable cyber incident to drive greater alignment with CISA's proposed definition of substantial cyber incident at §226.1. To this same end, we suggested that any Coast Guard requirement to report ransom payments should be harmonized with CISA's final rule to implement CIRCIA. AWO urges CISA to work closely with the Coast Guard as both agencies finalize their regulations to ensure the "substantial similarity" of definitions and reporting requirements to facilitate the adoption of a CIRCIA agreement.

Covered entities are only able to report available information and preserve available data and records.

AWO appreciates CISA's recognition of the fact that certain information regarding a covered cyber incident may be unavailable by the proposed 72-hour report deadline and certain information on ransom payments may not be available by the proposed 24-hour report deadline. We support the establishment of a supplemental reporting framework as proposed in §226.3(d) that allows for iterative compliance with CIRCIA, updating or supplementing a Covered Cyber Incident Report as new information becomes known. In line with this reasoning, AWO also supports the proposed §226.13 (b)(2) because it protects a covered entity from creating data or records it simply does not have for the sole purpose of fulfilling preservation requirements.

<u>Definitions</u>

The terms "covered cyber incident" and "substantial cyber incident" in proposed §226.1 are redundant and may be confusing for the regulated community. We recommend striking the term "covered cyber incident" and simply requiring covered entities to report substantial cyber incidents in proposed §226.3 and throughout the proposed regulations.

[3] Ibid.
[4] Ibid (footnote 37).

Again, AWO appreciates the opportunity to comment on the CIRCIA proposed rule and would be happy to provide more information as CISA sees fit.

Sincerely,

Caitlyn E. Stewart
Vice President – Regulatory Affairs