July 3, 2024

Cybersecurity and Infrastructure Security Agency
United States Department of Homeland Security
1110 N. Glebe Road
Arlington, VA 20598

Re: Notice of Proposed Rulemaking – Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Docket No. CISA-2022-0010)

The International Liquid Terminals Association (ILTA), submit these comments responding to the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements Notice of Proposed Rulemaking (NPRM) published by the Cybersecurity and Infrastructure Security Agency (CISA) in the Federal Register on April 04, 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. For this reason, CIRCIA's reporting requirements are of special interest to ILTA.

I. DEFINITIONS: 89 Fed. Reg. 23660

Comment – CISA is proposing definitions for a variety of terms that will have a specific meaning within the proposed regulation, therefore, CISA must clarify potentially confusing terms.

Recommendation – ILTA urges CISA to provide clear definitions and examples of any "covered cyber incident" and ''substantial cyber incident' that would meet the reporting threshold criteria consistent with other federal and state definitions of 'security incident(s)' or "authorized access' (actual v. potential). ILTA urges CISA to provide clear definitions and examples of any "covered entities" and "covered facilities, and they should be across sectors if not specific to each sector."

II. TIMING OF SUBMISSION OF CIRCIA REPORTS: 89 Fed. Reg. 23725

Comment – CISA's proposed reporting timeline is unrealistic and too short, as evidenced by CISA's delay in notifying the public about a cybersecurity intrusion that occurred in January.

Recommendation – CISA should allow Covered Entities not less than 96 hours to report an actual unauthorized security incident (v. a discovery of a potential risk) Covered Cyber Incident once a Covered Cyber Incident has been verified as having the reportable impact.

Please also note the timeline in informing affected entities of this intrusion. For example, on June 20, 2024, CISA issued an email notifying that the CSAT tool was the target of a cybersecurity intrusion by a malicious actor from January 23-24, 2024. It is unrealistic to expect tight reporting timelines when the agency requesting and enforcing those timelines cannot comply with similar reporting.

III. SUBSTANTIALLY SIMILAR REPORTING: 89 FED. REG. 23708

Comment – Industry owners and operators who are subject to other reporting regimes should be required to report qualified cyber incidents to only one agency, without CIRCIA's additional criteria.

Recommendation – ILTA urges CISA to harmonize with the other regulatory agencies and provide clear rationale for substantially similar reporting exceptions for industry owners and operators. CISA should share any reported information with necessary coordinating government agencies and relieve industry from duplicating reporting.

Industry owners and operators are subject to other reporting regulations, such as the Maritime Transportation Security Act of 2002 or Chemical Facility Anti-Terrorism Standards. Industry owners and operators should not be required to report qualified cyber incidents to both CISA and the National Response Center.

IV. EXCEPTIONS TO REQUIRED REPORTING ON COVERED CYBER INCIDENTS AND RANSOM PAYMENTS: 89 Fed. Reg. 23708

Comment – It is unclear whether CISA will permit any statutory exemptions to the CIRCIA.

Recommendation – CISA should clarify whether that it will allow statutory exemptions to CIRCIA. For example, CFATs and MTSA facilities should be exempt where reporting the same incidents according to similar reporting obligations with other federal agencies.

V. PURPOSE AND INTENT: 89 Fed. Reg. 23651

Purposes of the CIRCIA Regulation

Comment – ILTA shares CISA's intent to protect our Nation's Critical Infrastructure from adversaries who use the cyber domain to disrupt our operations, however, the specific intent of what the CIRCIA seeks to achieve remains unclear.

Recommendation – CISA must further clarify the intent and purpose of the rule and how it is stands separately from or compliments other rules.

VI. IMPACT ANALYSIS: 89 Fed. Reg. 23648

Comment – CISA estimated CIRCIA Reports over the period of analysis will result in $1.4 billion (undiscounted) in cost to industry, which is significant.

Recommendation – ILTA urges CISA to conduct a more thorough economic impact and cost analysis to implement this program.

VII. PROTECTING SENSITIVE INFORMATION

Comment – In light of CISA's recent hacking and repeated hacks of government systems, ILTA is concerned CISA will not adequately secure the information provided in a Covered Cyber Incident Report.

Recommendation – CISA should consider a form of air-gap or other strong security protocols for protection.

On June 20, 2024, CISA sent a notice that the CSAT tool was hacked. CISA recently confirmed that hackers likely accessed sensitive information about the nation's chemical facilities during the January cyberattack. ILTA believes that, over time, the government would likely collect and store thousands of instances of this critical cyber data in a single platform. ILTA is therefore concerned the government will not adequately secure the information industry reports. This critical information could be subject to state-sponsored or other adversaries. As such, CISA should enhance its security protocols or consider a form of air-gap for protection.

VIII. PRIVACY CONCERNS

Comment – Information that industry owners and operators report to CISA related to a Covered Cyber Incident risks impacting market stability and industry participant reputation.

Recommendation – Any information industry owners and operators report to CISA related to a Covered Cyber Incident should be exempted from the Freedom of Information Act or other methods of public disclosure to help preserve security and protect privacy.

IX. IMPLEMENTATION

Comment – The industry will need to be afforded the necessary time to build capacity to comply with the rule. The government will need time to build a safe system and a balanced and consistent enforcement scheme.

Recommendation – The CIRCIA rule should take effect not earlier than three (3) years from the final ruling.

Comment – The CIRCIA would be overly burdensome on small terminal operators.

Recommendation – CISA should grant an exception to owners and operators with facilities employing less than 10 full time employees.

***

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

Leakhena Swett
President
ILTA | International Liquid Terminals Association
703-851-2938
lswett@ILTA.ORG

Leakhena Swett