Proposed Rules

Federal Register
Vol. 89, No. 107
Monday, June 3, 2024

This section of the FEDERAL REGISTER contains notices to the public of the proposed issuance of rules and regulations. The purpose of these notices is to give interested persons an opportunity to participate in the rule making prior to the adoption of the final rules.

DEPARTMENT OF HOMELAND SECURITY

6 CFR Part 226

[Docket No. CISA–2022–0010]

RIN 1670–AA04

Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Correction

AGENCY: Cybersecurity and Infrastructure Security Agency, DHS.

ACTION: Proposed rule; correction.

SUMMARY: On April 4, 2024, the Cybersecurity and Infrastructure Security Agency (CISA) published, in the **Federal Register**, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements notice of proposed rulemaking (NPRM). The NPRM proposes regulations to implement CIRCIA's covered cyber incident and ransom payment reporting requirements for covered entities. In the section describing covered entities, the NPRM included information and references in the applicability criteria for transportation system entities that were based on a proposed rule that has not yet been published by the Transportation Security Administration (TSA). This document clarifies and corrects the proposed applicability criteria for pipeline facilities and systems in the sector-based criteria discussion for transportation systems sector entities.

DATES: Comments to the NPRM published at 89 FR 23644 on April 4, 2024, and related material must be submitted on or before July 3, 2024.

ADDRESSES: You may send comments, identified by docket number CISA–2022–0010, through the Federal eRulemaking Portal available at *https://www.regulations.gov.*

Instructions: All comments received must include the docket number for this rulemaking. All comments received will be posted to *https://www.regulations.gov,* including any personal information provided. If you cannot submit your comment using *https://www.regulations.gov,* contact the person in the **FOR FURTHER INFORMATION CONTACT** section of this proposed rule for alternate instructions. For detailed instructions on sending comments and additional information on the types of comments that are of particular interest to CISA for this proposed rulemaking, see the **SUPPLEMENTARY INFORMATION** section of the proposed rulemaking document at 89 FR 23644 (Apr. 4, 2024).

Docket: For access to the docket and to read background documents mentioned in this proposed rule and comments received, go to *https://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Todd Klessman, CIRCIA Rulemaking Team Lead, Cybersecurity and Infrastructure Security Agency, *circia@cisa.dhs.gov,* 202–964–6869.

SUPPLEMENTARY INFORMATION:

Background and Discussion

On April 4, 2024, CISA published a NPRM, ''Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements,'' 89 FR 23644, that was required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).[1] CIRCIA requires covered entities to report to CISA within certain prescribed timeframes any covered cyber incidents, ransom payments made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report.[2] CIRCIA further requires the Director of CISA to implement these new reporting requirements through rulemaking. The NPRM solicits public comment on proposed regulations that would codify these reporting requirements.

In proposed 6 CFR 226.2, Applicability, CISA proposed a list of entities that would be required to report under the proposed regulation.[3] Specifically, in § 226.2(b)(14), CISA proposed sector-based criteria for ''Transportation system entities'' that would be considered covered entities.[4] As noted in the NPRM, CISA aligned the aforementioned sector-based criteria's description of a covered entity to include those entities identified by TSA as requiring cyber incident reporting and, in some cases, enhanced cybersecurity measures.[5] To facilitate this alignment, CISA's NPRM proposed § 226.2(b)(14) that an ''entity required by the Transportation Security Administration to report cyber incidents'' or otherwise meets one or more criteria related to owners and operators of various non-maritime transportation system infrastructure, such as freight railroad, public transportation and passenger railroads (PTPR), pipeline facilities and systems, over-the-road bus (OTRB) operations, passenger and all-cargo aircraft, indirect air carriers, airports, and Certified Cargo Screening Facilities, would be considered a covered entity.[6] Each of these proposed criteria included specific references to where these entities are identified in TSA's current regulations.[7] However, for the sector-based criteria that would be applicable to pipeline facilities or systems, the proposed criterion references a section, 49 CFR 1586.101, that TSA intends to include in TSA's forthcoming Enhancing Surface Cyber Risk Management NPRM, which has not yet been published in the **Federal Register**.[8] Until that rule is finalized, the section related to pipeline facilities or systems does not exist in the CFR. Because the CIRCIA NPRM does not specifically describe which pipeline facilities or systems that CISA proposes as covered entities until TSA's rulemaking is finalized, CISA's intent through this notice is to clarify and correct this point.

As stated in the CIRCIA NPRM, CISA's intent is to align CIRCIA requirements applicable to aviation and surface transportation entities with TSA's requirements to support reduction of duplication and to avoid unintended gaps in cyber incident reporting. As such, CISA proposed applicability criteria describing covered entities in 6 CFR 226.2(b)(14) that include entities that are currently required, or will be required, to report

[1] See 6 U.S.C. 681–681g; Public Law 117–103, as amended by Public Law 117–263 (Dec. 23, 2022).

[2] 6 U.S.C. 681b(a)(1)–(3).

[3] 89 FR 23768 (Apr. 4, 2024).

[4] 89 FR 23768.

[5] *See* 89 FR 23699–23701.

[6] 89 FR 23768.

[7] *See* 89 FR 23768.

[8] *See* 89 FR 23768 and TSA, Fall 2023 Unified Agenda, RIN 1652–AA74: Enhancing Surface Cyber Risk Management, *https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202310RIN=1652-AA74* (accessed May 14, 2024).

cyber incidents to TSA.[9] It is for this reason that CISA specifically proposed describing a covered entity as an ''entity [that] is required by the Transportation Security Administration to report cyber incidents'' in proposed 6 CFR 226.2(b)(14), so that any entities, such as pipeline facilities or systems, that are required to currently report cyber incidents to TSA under Security Directives would also be considered covered entities that are required to report under CIRCIA.

For the surface transportation sector, TSA currently requires reporting of cyber incidents to CISA by owner/operators of certain freight railroads, passenger railroads, rail transit systems, and hazardous and natural gas pipeline facilities and systems pursuant to Security Directives issued under the authority of 49 U.S.C. 114(*l*)(2).[10] Under these Security Directives, TSA notifies owner/operators of pipeline facilities or systems directly if the requirements in the Security Directive are applicable to them. Using a risk-based approach, a small percentage within each mode of transportation are required to report cybersecurity incidents, but these entities represent a significant portion of capacity, throughput, and ridership for each of these modes. As indicated in the CIRCIA NPRM, and as described in this notice, CISA proposes that all such owners/operators of pipeline facilities and systems identified by TSA and required to report cybersecurity incidents pursuant to TSA Security Directives are considered covered entities under 6 CFR 226.2(b)(14) until TSA finalizes its Enhancing Surface Cyber Risk Management rule.

To address the concern regarding cross-referencing a regulatory section that does not currently exist, CISA is issuing this correction to remove the reference to that specific regulatory section and, instead, propose criterion to make clear that CIRCIA's description of a covered entity for pipeline facilities or systems includes any entity that is currently required by TSA to report cyber incidents under a Security Directive or is otherwise identified as required to report under TSA's final regulations. For owner/operators of pipeline facilities or systems not currently subject to reporting requirements under TSA's Security Directives, it is CISA's understanding, through consultation with TSA, that TSA intends to continue using a risk-based approach in determining entities subject to its regulations, similar to its Security Directive approach and that applicability of cyber incident reporting requirements beyond the existing Security Directives will not be substantially expanded. TSA's Security Directives indicate that approximately 100 pipeline systems are considered the most critical.[11] CISA acknowledges the total number of owner/operators may slightly change consistent with an updated risk analysis developed for purposes of TSA's proposed rule. However, CISA continues to believe the Regulatory Impact Analysis for the CIRCIA rulemaking is an accurate estimate insomuch that the applicability of the TSA covered entities will continue to be approximately 115 entities.[12]

As mentioned in the CIRCIA NPRM, CISA believes that aligning CIRCIA's Applicability section with the population of entities from which TSA requires cyber incident reporting or at which TSA requires the implementation of enhanced cybersecurity measures is appropriate for CIRCIA and consistent with the factors contained in 6 U.S.C. 681b(c)(1). CISA will continue to coordinate with TSA throughout the rulemaking process to harmonize CIRCIA's Applicability section with TSA, to the maximum extent practicable.

Comments on the NPRM and related material must be submitted on or before July 3, 2024. *See* Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements; Extension of Comment Period at 89 FR 37141. DHS believes this correction does not warrant extending the current 90-day comment period for the NPRM.

Correction

■ In FR Doc. 2024–06526, published at 89 FR 23644 in the issue of April 4, 2024, on page 23768, in the third column, in § 226.2, correct paragraph (b)(14)(iv) to read as follows:

§ 226.2 [Corrected]

* * * * *

(b) * * *

(14) * * *

(iv) A pipeline facility or system owner or operator required to report cyber incidents by the Transportation Security Administration;

* * * * *

Jennie M. Easterly,

Director, Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

[FR Doc. 2024–12084 Filed 5–30–24; 8:45 am]

BILLING CODE 9111–LF–P

[9] 89 FR 23768.

[10] *See* 89 FR 23651.

[11] *See* TSA Security Directive Pipeline-2021–02D, at 4 n.9 (citing section 1557(b) of the Implementing Recommendations of the 9/11 Commission Act of 2007, Public Law 110–53 121 Stat. 266, 475 (codified at 6 U.S.C. 1207(b)).

[12] *See* Section 2.2.14 of the Preliminary RIA, which estimates 115 pipeline entities would be affected by the proposed criteria for pipeline facilities or systems.

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 165

[Docket Number USCG–2024–0449]

RIN 1625–AA00

Safety Zone; Fireworks Display, Marina Park, Irrigon, OR

AGENCY: Coast Guard, DHS.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Coast Guard is proposing to establish a temporary safety zone for certain waters of Umatilla Marina. This action is necessary to provide for the safety of life on these navigable waters near Irrigon, OR, during a fireworks display on July 27, 2024. This proposed rulemaking would prohibit persons and vessels from entering the safety zone unless authorized by the Captain of the Port Columbia River or a designated representative. We invite your comments on this proposed rulemaking.

DATES: Comments and related material must be received by the Coast Guard on or before July 3, 2024.

ADDRESSES: You may submit comments identified by docket number USCG–2024–0449 using the Federal Decision-Making Portal at *https://www.regulations.gov.* See the ''Public Participation and Request for Comments'' portion of the **SUPPLEMENTARY INFORMATION** section for further instructions on submitting comments. This notice of proposed rulemaking with its plain-language, 100-word-or-less proposed rule summary will be available in this same docket.

FOR FURTHER INFORMATION CONTACT: If you have questions about this proposed rulemaking, call or email Lieutenant Carlie Gilligan, Waterways Management Division, Marine Safety Unit Portland, Coast Guard; telephone 503–240–9319, email *SCRWWM@USCG.MIL.*

SUPPLEMENTARY INFORMATION:

I. Table of Abbreviations

CFR Code of Federal Regulations
COTP Captain of the Port