ASSOCIATION OF AMERICAN RAILROADS

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

July 3, 2024

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
Washington, DC 20528

Re: Notice of Proposed Rulemaking (NPRM), Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS); Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements (Docket No. CISA–2022–0010; 89 *Federal Register (FR)* 23644, April 4, 2024)

Dear Director Easterly:

The Association of American Railroads (AAR) and the American Short Line and Regional Railroad Association (ASLRRA) (collectively, the Associations) respectfully submit the following comments in response to CISA's NPRM on CIRCIA Reporting Requirements. CIRCIA directed CISA to define several critical elements of new regulations, including which organizations will be "covered entities" that must report cyber incidents, what types of cyber incidents must be reported, and the scope of proposed retention requirements. However, the proposed rule takes an expansive approach to each of these proposed definitions, and, as such, the definitions should be refined and narrowed. In addition, CISA should reduce the scope of proposed retention requirements and undertake efforts to promote harmonization with other reporting requirements from other agencies.

ASSOCIATION OF AMERICAN RAILROADS

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

The Associations offer the perspective and experience of the rail sector, which has been operating under various and changing security directives issued by the Transportation Security Agency (TSA) under asserted emergency authority since 2021.[1] These security directives include mandatory cyber incident reporting with a 24-hour deadline. The rail industry's experience with the security directives and TSA reporting should inform CISA's consideration of new reporting obligations that may be burdensome and duplicative of those required by other agencies.[2] CISA should work to reduce burdens and advance alignment and harmonization of reporting obligations, in a transparent manner that considers burdens and benefits.

I. The Proposed Definition of "Covered Entities" Is Overly Broad and Exceeds the Intent of Congress, and It Should Be Revised Accordingly.

The proposed rule contains an overbroad definition of "covered entities."[3] Specifically, CISA proposes applying the definition to any entity in the Transportation Sector that exceeds a small business threshold.[4] Further, for those entities not meeting this threshold, CISA would

---

[1] *See*, *e.g.*, SD 1580-21-01 – Enhancing Rail Cybersecurity; SD 1580/82-2022-0 – Rail Cybersecurity Mitigation Actions and Testing1; SD 1580/82-2022-01 - Rail Cybersecurity Mitigation Actions and Testing (correction memo); SD 1580-21-01A – Enhancing Rail Cybersecurity; SD 1580-21-01 – Enhancing Rail Cybersecurity (correction memo); SD 1580_1582-2022-01A – Rail Cybersecurity Mitigation Actions and Testing; SD 1580-21-01B – Enhancing Rail Cybersecurity, all of which are available at www.tsa.gov/sd-and-ea.

[2] Currently, TSA, through the issuance of security directives, requires the reporting of cybersecurity incidents to CISA. TSA should not require any reporting once CISA finalizes its rule. Congress intended CISA, not TSA, to regulate the reporting of cyber security incidents.

[3] CISA interprets the word "entity" to include "any person, partnership, business, association, corporation, or other organization (whether for-profit, not-for-profit, nonprofit, or government). . . ." Because of this interpretation, there is confusion as to whether associations, like AAR and ASLRRA, would be considered "covered entities" that are required to report cyber incidents to CISA under the proposed rule. A clarification is needed to ensure that associations are not inadvertently covered by the regulation.

[4] *See* proposed §226.2(a), NPRM at 23767.

ASSOCIATION OF AMERICAN RAILROADS

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

apply sector-based criteria.[5] As concerns the freight rail industry, this would include any freight railroad carrier identified in 49 CFR 1580.1(a)(1), (4), or (5), as well as any entity already required by TSA to report cyber incidents.[6]

Until now, TSA has only required freight railroads that fall under 49 CFR 1580.101, and a select number of other carriers they identified—approximately 70 covered entities—to comply with the series of rail cybersecurity directives issued by TSA since 2021.[7] The proposed rule would drastically increase that scope to include all freight railroads, including all of the more than 600 Class II and III railroads, the majority of which TSA has not seen cause to regulate and would otherwise not be large enough to exceed the proposed small business threshold.

In addition, CISA has proposed that a covered entity constitutes "the *entire* entity" and is not limited to the "individual facilities or functions."[8] In other words, if one part of an entity's operations is deemed to be in critical infrastructure, the entire entity will be subject to CISA's cyber incident reporting requirements. In addition, "unauthorized access" to data hosted by a third-party provider "caused by a compromise of . . . [the] third-party data hosting provider" could be interpreted as part of a covered entity's "information system or network," thereby further complicating what is to be deemed part of a "covered entity."[9]

---

5 *See id*.

6 *See* proposed §226.2(b)(14), NPRM at 23768.

7 SD 1580-21-01B, SD 1582-21-01B and SD 1580_1580-2022-01B are the most recent versions in the series

8 *See* proposed §226.2(b)(14), NPRM at 23768 (emphasis added).

9 *Id.*

ASSOCIATION OF AMERICAN RAILROADS

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

As a result of the overexpansive definition of "covered entity," CISA's proposal will result in duplicative and excessive reporting; under the proposed rule, entities already reporting to CISA under the TSA security directives would also be required to report to CISA *under this regulation* but on a far broader scope—despite CISA's repeatedly stated intention to align the CIRCIA requirements applicable to surface transportation entities with TSA's requirements.[10] Having two requirements to report *to the exact same agency* makes little sense and only creates opportunities for confusion, especially given the distinct reporting requirements in the different mandates. Moreover, covered entities' business functions that are not critical infrastructure functions would be subject to reporting under the proposed rules. This needlessly duplicative and unnecessary reporting will result in too many reports. The influx of these reports will hamstring CISA's ability to rapidly and effectively analyze threat information and share defensive measures with the rail industry in a timely fashion.

This is plainly against congressional intent. At a May 1, 2024, congressional hearing, the House Homeland Security Committee expressed Congress's desire that CIRCIA reporting not become all encompassing.[11] For example, Rep. Yvette Clarke (D-NY) stated that Congress "did not intend to subject everyone or every incident to reporting."[12] To the contrary, she explained that it was Congress's "intent . . . that reporting requirements would be appropriately tailored

---

[10] See 89 FR 47471.

[11] *See* https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposed-rulemaking/.

[12] *Id.*

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

to limit overreporting. . . ."[13] Rep. Eric Swalwell (D-CA) echoed Rep Clarke's sentiments, warning that the proposed reporting requirements may never reach their full potential because CIRCIA, like the Automated Indicator Sharing (AIS) program before it, focuses too much on "quantity over quality."[14]

CISA's NPRM appears to discount the risk of overreporting without meaningful engagement or an explanation of how the agency will meaningfully analyze and use the vast array of reports it will receive.[15] This makes its proposed cost-benefit analysis deeply flawed as well, because it supposes benefits from extensive reporting by hundreds of thousands of entities across the United States—and likely undercounts covered entities as well.

Accordingly, CISA should reframe the definition of "covered entity" to a smaller set of critical infrastructure entities and take a risk-based approach to doing so.[16] At a minimum, CISA should limit its definition of covered entities in the rail sector to those currently required to report incidents under the existing TSA security directives, similar to CISA's approach to the pipeline sector. In addition, CISA should also limit reporting requirements to those business functions that are engaged in critical infrastructure. Adjustments like these would reduce the number of reports that CISA is likely to receive and, in turn, make it more likely that CISA can evaluate and share timely and valuable information from the mandatory reports.

---

13 *Id.*

14 *Id.*

15 *See* 89 FR 23661.

16 *See* AAR Comments, Request of Information on the Cyber incident Reporting for Critical Infrastructure Act of 2022, CISA-2022-0010, at 6-7 (Nov. 14, 2022) ("AAR RFI Comments").

ASSOCIATION OF AMERICAN RAILROADS

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

II. The Definition of "Substantial" Cyber Incidents Is Vague and May Be Read Too Broadly; CISA Should Limit the Scope of the Definition.

Like the proposed definition of "covered entities," the proposed definition of "substantial cyber incidents" could be read too broadly, as "substantial" is largely an undefined term and does not modify all the factors that may make something a covered incident. The proposed definition of "substantial cyber incidents" should be narrowed by adding language to the "unauthorized access" prong to require a "demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety." The potential for confusion is exacerbated by vague and overinclusive language.

The proposed rule would be additionally improved by revisions to the third party-data provider and supply chain prong of its definition of "substantial" to also include a significant threshold. Third-party incidents present their own challenges for covered entities because it can take time to obtain details from third parties that are having an incident, and there may be contractual or confidentiality issues related to the sharing of information. Covered entities may rely on an array of third parties—large and small—for various services, technology, and functions. However, the proposed rule does not focus on critical third parties whose incidents may have a serious impact on a covered entity; nor does the proposal tie covered third-party incidents to any harm or impact threshold. The third-party triggers should be removed or substantially changed to focus on vendors the covered entity has deemed critical, and to

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

include substantiality thresholds such that minor events affecting third parties do not cause an onslaught of reports to the government.

Once again, CISA's broad approach runs contrary to the intent of Congress. At the May 1, 2024 hearing, Representatives on the Homeland Security Committee confirmed that it was Congress's intent to only require reporting of incidents that meet an impact threshold.[17] Indeed, CISA's Director indicated that it is important to focus efforts on "signals, not noise."[18] As AAR suggested previously in response to the RFI, reportable incidents should be limited to *significant* incidents that have a reasonable likelihood of disrupting the operations of the critical infrastructure entity.[19] In the case of railroads, this would mean only those incidents that would significantly disrupt the movement of trains throughout the North American network. Accordingly, in order to promote ease of administration and to reduce unnecessary overreporting, CISA should endeavor to avoid such confusion by removing vague language and revising the "disruption" prong of its definition of "substantial" covered incidents to include a threshold that is both harm-based and clear.[20]

These changes will ensure that covered entities have certain and limited required reporting that is closer to the goals of Congress in adopting CIRCIA. This will reduce the number

---

[17] *See* https://homeland.house.gov/hearing/surveying-circia-sector-perspectives-on-the-notice-of-proposed-rulemaking/.

[18] Samantha Schwartz, *What incident reporting could look like*¸ Cybersecurity Dive, Dec. 10, 2021, *available at* https://www.cybersecuritydive.com/news/incident-reporting-law-mandatory-cisa-fbi/611254/.

[19] *See* AAR RFI Comments, at 7.

[20] Proposed §226.3(d), NPRM at 23769.

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

of superfluous reports that CISA is likely to receive and, in turn, make it more likely that CISA can produce valuable information that "enhance[s] situational awareness of cybersecurity threats across critical infrastructure sectors."[21]

III. Information Required to Be Reported in CIRCIA Reports Is Excessively Broad, as Is the Supplementation Obligation.

Sections 226.8-11 of the proposed rule would require the reporting of broad and often undefined sets of information, including language such as "*any* information," "*any* vulnerabilities," and "*any* indicators."[22] These sections also make frequent use of the phrase "including but not limited to," which is certain to create confusion regarding the outer boundaries of what covered entities are required to report.[23]

The rail sector has been operating under security directives that require reporting of cyber incidents and offers CISA some observations based on members' experience. The reporting under the Security Directives already imposes substantial burdens on operators. It is often difficult to obtain and confirm the mandated information within the short 24-hour period required under the security directives, and to develop answers to the many questions on the CISA form. Completing the form takes valuable time from companies' security operators and their legal teams. The questions on that form differ substantially from the information proposed to be reported in new Section 226.8. CISA's form presently asks for substantial

---

21 6 U.S.C. § 669(c)(13).

22 Proposed §§226.8(b), (c), (f), NPRM at 23770-71 (emphasis added).

23 *See, e.g.,* proposed §§226.8(a), (a)(1), (a)(3), (c), (d), (e), (f), (h), (i), (i)(3), NPRM at 23770-71.

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

amounts of information, and it has proven challenging in many respects. Some fields require predictions and estimates that simply may not be reasonably made at the 24-hour mark.[24] Some fields have proven not to be relevant or applicable to some incidents, resulting in wasted time considering how to parse an agency definition and develop an answer. The form classifies incidents and systems in ways that may not align with operators' system classifications.[25] These are just a few examples of how the current reporting mandate creates challenges. The information that CISA proposes to require would eclipse this and impose substantially more burdens on operators' security and legal teams to gather, package, review, and verify required information. The NPRM's supplementation requirement will compound these challenges because the trigger for required supplementation is not clear and it may entail updating all the information previously reported, at unclear cadences, as some of the required factual elements in Section 226.8 are destined to change and evolve over an incident and its response and evaluation.

AAR's members report that, despite making incident reports to the government under the Security Directives, they rarely if ever receive actionable information or responses. CISA should consider carefully the effectiveness, utility, and substantial burden of the current reporting mandate as it considers how to implement CIRCIA. The agency should work to

[24] The form asks for the "estimated recovery time" in hours and days, which may not be predictable to any reasonable certainty at 24 hours.

[25] For example, it requires submitters to answer "where was the activity observed" and then provides seven options: Business DMZ; Business Network Unknown; Business Network Management; Critical System DMZ; Critical System Management; Critical Systems; and Safety Systems.

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

minimize burdens on operators and align reporting obligations. As discussed below, CISA should streamline and reduce the information required in Section 226.8, and DHS and TSA should eliminate the mandates for rail in the security directives, or, at a minimum, harmonize them by providing rail reporting mandate a minimum of 72 hours.

IV. CISA Should Reduce the Scope of Proposed Retention Requirements.

The proposed rule would require covered entities to preserve numerous types, and large volumes, of information related to a covered incident, including communications with any threat actor (*e.g.*, copies of actual correspondence), indicators of compromise, log entries (*e.g.*, DNS, firewall, packet capture, endpoint, or Active Directory), "relevant forensic artifacts" such as forensic images or preserved hosts, network data, data and information "that may help identify" how a threat actor compromised a system, system information to identify exploited vulnerabilities (*e.g.*, operating systems, version numbers, patch levels, and configuration settings), information about any exfiltrated data, data or records related to paying a ransom, and any forensic or other reports about an incident (such as those created by a cybersecurity services vendor).[26] Further, data must be preserved for two years, and this period may be extended upon the discovery of "substantial new or different information."[27] The records and data must be preserved in their original format and form, and must be "readily accessible,

[26] NPRM at 23732.

[27] *Id.*

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

retrievable, and capable of being lawfully shared by the covered entity in response to a lawful government request."[28]

This information is voluminous and will impose significant costs to store and retain. Accordingly, CISA should limit the retention requirement to records sufficient to assess whether a covered entity appropriately determined that an incident was "covered." And it should do this while also limiting the scope of covered incidents, to limit unnecessary retention of data of dubious relevance and importance.

V. CISA Should Interpret the "Substantially Similar" Requirement More Broadly to Promote Harmonization and Eliminate Duplicative Reporting.

Harmonization of incident reporting requirements under CIRCIA was, and continues to be, one of Congress' key cybersecurity priorities.[29] As noted above in Section I, under the NPRM, the definition of "covered entity" encompasses any entity already required by the Transportation Security Administration (TSA) to report cyber incidents.[30] And CISA recognizes the need for harmonization of cyber incident reporting.[31] Indeed, CISA has "engag[ed] with other Federal departments and agencies that implement cyber incident reporting requirements

---

28 *Id.*

29 Letter of Homeland Security Chairman Mark E. Green, MD (R-TN) and Subcommittee on Cybersecurity and Infrastructure Protection Chairman Andrew Garbarino (R-NY) letter to SEC Chair Gary Gensler on duplicative SEC incident reporting rule, Sept. 5, 2023.

30 Proposed §226.2(b)(14), NPRM at 23768.

31 *See* NPRM at 23653.

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

to determine whether covered entities could potentially take advantage of the proposed substantially similar reporting exception to CIRCIA reporting."[32]

"To qualify for the substantially similar reporting exception, the information reported by a covered entity on a covered cyber incident or ransom payment to another Federal agency must be substantially similar to the information that the covered entity would be required (but for the exception) to report to CISA . . . ."[33] Concerningly, however, "CISA does not intend to define what constitutes substantially similar information in the final rule."[34]

Under the TSA Security Directive, freight rail carriers' incident reporting obligations are required for incidents involving "the freight railroad carrier's Information or Operational Technology systems or other aspect of the Owner/Operator's rail systems or facilities the Owner/Operator has responsibility to operate and/or maintain." By contrast, the scope of the proposed CIRCIA rules would apply to far more than a freight railroad's rail systems or facilities by extending the obligation to non-critical infrastructure assets and information. This broad scope may prevent harmonization between the CIRCIA rules and the TSA Security Directive on incident reporting, if the government deems the type of incidents covered to be too different, or the reportable information is not seen as substantially similar. The TSA Security Directive already requires freight railroads to report cyber incidents to CISA using the CISA Incident Reporting Form within 24 hours. Accordingly, the Security Directive and the forthcoming

---

32 *Id*.

33 *Id.* at 23709.

34 *Id.*

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

CIRCIA rules present what should be an ideal opportunity for elimination of the requirements under the security directives, or, at the very least, harmonization. Given that the TSA reporting under the security directives is only *temporary*, CISA should work with TSA to eliminate the reporting requirements from the TSA security directives, instead of requiring reporting under both the TSA security directives and CIRCIA *to the same agency*, as well as future rulemakings.[35] At a minimum, CISA should clarify that a freight railroad that reports under TSA's security directives would be deemed to have satisfied the reporting requirements under CIRCIA.

CONCLUSION

The proposed rule would include too many entities and too many incidents, and it seeks to collect and require retention of too much information. Unless addressed, these issues will result in excessive and superfluous reports, which will hamper CISA's ability to analyze threats and share defensive measures with the speed and accuracy that would make such information valuable. Furthermore, burdensome retention requirements and unclear harmonization guidelines will impose significant expense on businesses, like freight railroads. A final rule that

[35] CISA NPRM correction, 89 FR 47471 (June 3, 2024).

ASSOCIATION OF AMERICAN RAILROADS

Amber L. McDonald
Assistant General Counsel
amcdonald@aar.org
(202) 639-2507

embraces more targeted reporting requirements and greater harmonization will ultimately result in fewer unnecessary burdens and greater utility from the information shared.

Respectfully submitted,

Kathryn D. Kirmayer
J. Frederick Miller Jr.
Amber L. McDonald
Association of American Railroads
425 Third Street, S.W., Suite 1000
Washington, DC 20024

Counsel for the Association of American Railroads

Sarah Yurasko
American Short Line and Regional Railroad Association
50 F Street N.W., Suite 500
Washington, DC 20001

Counsel for the American Short Line and Regional Railroad Association