BEFORE THE
CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Docket No. CISA–2022–0010

CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT REPORTING REQUIREMENTS

SUPPLEMENTAL COMMENTS OF THE AMERICAN SHORT LINE AND REGIONAL RAILROAD ASSOCIATION

The American Short Line and Regional Railroad Association ("ASLRRA"), on behalf of itself and its member railroads, submits these comments to supplement oral testimony provided at the Cybersecurity and Infrastructure Security Agency ("CISA") town hall meeting on June 16, 2026, to discuss the notice of proposed rulemaking ("NPRM") on Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") Reporting Requirements.[1] 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.[2] As shared during the town hall, ASLRRA advocates that CISA modify the proposed applicability of the CIRCIA rule to harmonize with the Transportation Security Administration's ("TSA") applicability criteria.

ASLRRA is a small non-profit trade association representing over 500 Class II and Class III railroads ("short lines"). Short lines operate nearly 50,000 route miles in the United States, or

---

[1] 91 Fed Reg. 30,498 (May 26, 2026). ASLRRA submits these supplemental comments directly to CISA via circia@cisa.dhs.gov within seven calendar days of the town hall session as per the instructions provided to town hall participants.

[2] 89 Fed. Reg. 23,644 (April 4, 2024).

approximately 30% of the national freight network, touching in origin or destination one out of every five cars moving on the national railroad system, serving customers who otherwise would be cut off from the national railroad network. Both in legislative matters before Congress, and in regulatory matters before state and federal agencies, ASLRRA advocates for enlightened public policies which promote a strong short line rail component for the national transportation infrastructure. Most short line railroads are considered small businesses.[3] ASLRRA's members stand to be impacted by this proposed rule if they are swept in as "covered entities" that must report cyber incidents.

BACKGROUND

ASLRRA submitted comments in response to the NPRM jointly with the Association of American Railroads ("AAR," jointly, "the Associations") on July 3, 2024.[4] In those comments, the Associations provided that the proposed rule would include too many entities and too many incidents and 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. Specifically, the Associations stated that the proposed definition of "covered entities" is overly broad and exceeds the intent of Congress; the definition of "substantial" cyber incidents is vague and may be read too broadly, information required to be reported in CIRCIA reports as well as the supplementation obligation is too excessively broad, CISA should reduce the scope of proposed retention requirements, and that CISA should

[3] *See* 13 C.F.R. § 121.201 and North American Industry Classification System code 482112, "Short Line Railroad."

[4] *See* ASLRRA and AAR Comments, Cyber Incident Reporting for Critical Infrastructure Act Reporting Requirements, CISA-2022-0010-0354 (July 3, 2024) ("Association Comments").

interpret the "substantially similar" requirement more broadly to promote harmonization and eliminate duplicative reporting.

Fred Oeslner, ASLRRA Vice President of Data, Technology and Security, provided testimony at the town hall meeting representing the concerns of short lines. His remarks focused on: (1) the proposed definition of "covered entities," which threatens to encompass all freight railroads in the nation, lacking harmonization with TSA's applicable criteria and risking confusion and unwarranted cost to small businesses; and (2) overly broad language related to the reporting of third-party incident to CISA.

I. The Definition of "Covered Entities" is Overly Broad and Should be Narrowed.

While CISA staff during the town hall represented during the town hall that the definition of "covered entities" would be consistent with TSA's definition, this is not mirrored by the language in the NPRM. The NPRM includes an overbroad definition of "covered entities." Specifically, CISA proposes applying the definition to any entity in the Transportation Sector that exceeds a small business threshold.[5] Further, for those entities not meeting this threshold, the NPRM would apply sector-based criteria.[6] 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.[7] As explained in the Associations' comments, TSA has traditionally only required freight railroads that fall under 49 CFR 1580.101, and a select number of other carriers they identified, to comply with the three series of rail cybersecurity directives issued by TSA since 2021, which amounts to approximately 70 covered

---

5 *See* proposed § 226.2(a), NPRM at 23767.

6 *See id*.

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

entities.[8] The proposed rule would drastically increase that scope to include all freight railroads, including all of the over 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.[9] CISA should refine and narrow the definition of "covered entities" in the NPRM by removing the reference to 49 CFR 1580.1(a)(1), (4), or (5), from the existing definition of "transportation system entities." This would harmonize the applicability of the rule with TSA's security directives and NPRM.

A. TSA's Definition of "Covered Entities" for Cyber Incident Reporting is Narrower than the proposed definition in the CIRCIA NPRM.

The applicability of the TSA security directives and TSA's NPRM to Class II and III freight railroads differ from each other, with the NPRM applicability scope expanding from that in the security directives, but both definitions of applicability are significantly narrower than what is proposed in the CIRCIA NPRM.

i. The TSA Security Directive Coverage is Limited to Only Some Short Lines

Since late 2021, TSA has published two series of security directives (SD 1580-21-01 and SD 1580/82-2022-01) that are applicable to some, but not all, short lines. The first series, SD 1580-21-01, most recently reissued as SD 1580-21-01E on January 9, 2026, initially identified freight railroad carriers identified in 49 CFR 1580.101 as those covered by the directive, with additional applicability for "other TSA-designated freight railroads" included in subsequent

[8] *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 on the DHS website at https://www.tsa.gov/sd-and-ea.

[9] *See* Associations' comments, pp. 2-3.

reissued versions.[10] This amended applicability is defined in the same manner as applicability in the second series of security directives, SD 1580/82-2022-01, which was most recently reissued as SD 1580/82-2022-01E, on May 3, 2026.[11]

Under the portion of the applicability definition from the security directives related to 49 CFR 1580.101, only a limited number of short lines meeting the definitions under subparts B or C are required to adhere to the security directives. Most short lines falling under this applicability category do so because they transport Rail Sensitive-Security Materials ("RSSM") through a High Threat Urban Area ("HTUA").[12] RSSMs are highly dangerous materials meeting explosive, radioactive or poisonous-by-inhalation standards that are beyond normal standards for hazardous materials. HTUAs represent 30 large cities, and their surrounding regions, through which the transport of RSSMs reflects a particularly high security risk due to the potential for a mass casualty incident related to their detonation or release. For security reasons, TSA does not publish the list of railroads who fall under this classification, but TSA staff advises that it is about 30 short lines.

TSA's second applicability category is less explicitly defined and is based on the broad powers TSA holds to issue security directives to any infrastructure service provider under its authority. TSA staff has advised that the other short lines covered by the security directives are those who are designated the Department of War's ("DOW") Military Surface Deployment and Distribution Command ("SDDC") as defense connector lines. Defense connector lines are those

[10] TSA, Security Directive 1580-2021-01E, Accessed June 22, 2026, https://www.tsa.gov/sites/default/files/signed_security-directive-1580-21-01e-and-transmittal-memo_508c.pdf.

[11] TSA, Security Directive 1580/82-2022-01E, Accessed June 22, 2026, https://www.tsa.gov/sites/default/files/signed_security_directive_1580_82-2022 01e_and_transmittal_memo_508c.pdf.

[12] See 49 C.F.R. § 1580.3.

that connect key DOW bases and facilities, or ports that could be utilized by DOW, to the broader Strategic Rail Corridor Network that constitutes the civil rail lines identified as critical for transporting military shipments and are primarily owned and operated by the larger Class I railroads.

Between the two applicability categories, TSA has indicated that they are regulating around 70 railroads under the security directives. Removing the Class I railroads from that pool would leave roughly 64 railroads, or approximately 10% of the nation's 600+ Class II and III freight railroads currently included as covered entities under the definition in the CIRCIA NPRM.

ii. The TSA NPRM Covers More Short Lines but Less than the CIRCIA NPRM

On November 7, 2024, TSA issued an NPRM, *Enhancing Surface Cyber Risk Management*.[13] This NPRM expands applicability to a wider range of railroads, but still significantly less than proposed in the CIRCIA rulemaking. Although the proposed rule includes language that would exclude the majority of short lines from many of the cyber risk management requirements, several provisions have the potential to needlessly envelop railroads with operations that do not represent a security risk to their localities or the national network. For example, the NPRM proposes to include all Class II and III railroads with annual operations in excess of 400,000 train miles.[14] This provision is based on an incorrect assumption that these railroads operate on such a scale that an operational interruption would significantly impact the flow of freight across the national network. As shared in ASLRRA's comments to the NPRM, at the 400,000 train-mile threshold, a short line could be included under the proposed rule, despite

[13] 89 Fed. Reg. 88,488 (Nov. 7. 2024).

[14] *See* 89 Fed. Reg. at 88,508.

only operating 2% of the miles that the smallest Class I operated.[15] The NPRM also proposes to include railroads with switching and terminal operations served by more than one Class I railroad.[16]

The Associations' comments highlight that expansion being overly broad from a security risk perspective. The train-mile threshold encompasses railroads orders of magnitude smaller than the Class Is without justifying why a cyber incident on those railroads poses a national security risk based solely on their size. The Associations' comments also urged TSA to limit the inclusion of railroads interchanging with multiple Class I carriers to only those whose operational disruptions could have national-level impacts, rather than broadly encompassing the many small short lines that interchange with multiple Class I carriers solely to provide their customers with more flexible shipping options, which is not indicative of their size or significance to the national freight network. ASLRRA estimates that these two provisions would increase the scope of the regulatory requirements to an additional 150 short lines. Nevertheless, even as currently written, the applicability criteria included in the TSA NPRM would apply to a far smaller set of Class II and III railroads than is defined in the CIRCIA NPRM, which would include over 600 freight railroads.

II. CISA Should Narrow the Scope of the Requirements to Report Third-Party Incidents.

At the town hall, Mr. Oelsner reiterated the position expressed in the Associations' comments to the CIRCIA NPRM, stating that third-party reporting should only be required for systems deemed by railroads to be critical to their operations as railroads. This is particularly important for short lines, which are more dependent than Class I freight railroads or larger

[15] *See* ASLRRA and AAR's comments at Docket No. TSA 2022-0010-0037.

[16] *See* 89 Fed. Reg. at 88,508.

passenger operations on third-party IT service providers for services whose disruption may not have a meaningful impact on rail operations. On the expansion of reporting requirements to all short lines, CISA staff indicated that the proposed rule did not actually intend to expand the reporting requirement beyond the short lines selected for cybersecurity oversight in the TSA security directives or the TSA NPRM. However, based on further review of the CIRCIA NPRM, ASLRRA remains concerned that the language would in fact include all short lines, which is significantly broader coverage than either the TSA security directives or proposed rulemaking.

CONCLUSION

ASLRRA advocates that CISA refine and narrow the definition of "covered entities" and clarify that third-party reporting should only be required for systems deemed by railroads to be critical to their operations as railroads, consistent with TSA's applicability criteria, delineated in the current security directives and the proposed surface cybersecurity rule.

ASLRRA appreciates the opportunity to present the concerns of short line freight railroads on this critical issue.

Respectfully submitted,

Sarah G. Yurasko
SVP–Law and General Counsel
American Short Line and Regional Railroad Association
50 F Street, NW, Suite 500
Washington, DC 20001

June 23, 2026