American
Public Transportation
Association

1300 I Street NW
Suite 1200 East
Washington, DC 20005
p: (202) 496-4800
f: (202) 496-4324

APTA.COM

July 2, 2024

Todd Klessman
CIRCIA Rulemaking Team Lead
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Subject: Docket No. CISA-2022-0010

Dear CIRCIA Rulemaking Team:

The American Public Transportation Association (APTA) represents a $79 billion industry that directly employs 430,000 people and supports millions of private-sector jobs. Safety is the number one core value of the public transportation industry, including bus, rail, commuter and intercity rail and ferry operators. The employees responsible for managing and operating public transportation systems are fully committed to the safety and security of their systems, passengers, fellow employees, and the public.

We appreciate the ongoing dialogue between the Cybersecurity and Infrastructure Security Administration (CISA) and APTA regarding critical infrastructure security. We also appreciate the opportunity to respond to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Notice of Proposed Rulemaking published in the *Federal Register* at 89 FR 23644 on April 4, 2024.

The Transportation Security Administration (TSA) imposed heightened cybersecurity requirements on some Mass Transit and Passenger Rail owners and operators through a series of Security Directives 1582-21-01 starting in December 2021.

Harmonization:

APTA members are concerned about the potential negative impacts of unharmonized, complex, and duplicative reporting regimes. APTA urges CISA to align CIRCIA's applicability section with the population of entities that TSA requires cyber incident reporting from. APTA urges CISA to coordinate with TSA throughout the rulemaking process of TSA's Enhancing Surface Cyber Risk Management notice of proposed rulemaking (NPRM) to harmonize CIRCIA's "applicability" section with TSA's.

Reporting:

Streamlining the reporting processes under CIRCIA is crucial for ensuring that agencies can report cyber incidents efficiently and effectively.

User-friendly, intuitively designed reporting that allows agencies to submit their incident and supplemental reports easily should be developed. Clear instructions, user support features such as templates or pre-filled forms, and step-by-step guidance to minimize errors and ensure comprehensive data collection should be employed. Features like autofill for previously entered information, drop-down menus for common incident types, and the ability to save and return draft reports should be considered.

Implementing a standardized incident and supplemental reporting format is critical to ensure consistency in the data collected and enable the analysis of cyber threats. APTA's members believe clarity is needed regarding when an owner/operator is expected to report an incident caused by a vendor, contractor or in the supply chain. In many cases, the covered entity has limited visibility into what happened with the contractor, vendor or along the supply chain to cause the incident. Clarifying this would ensure that covered entities are not unduly burdened with reporting obligations for incidents outside of their control but within the control of their contractors, vendors or in the supply chain.

APTA encourages CISA to make additional methods of reporting available. Reporting should not require the download or purchase of new technology. In addition, APTA recommends that CISA assign reference numbers to each report, which would allow entities to locate and return to a specific CIRCIA Incident Reporting Form at a later point. APTA also recommends that CISA not penalize entities for reporting in good faith under the rule. CISA should avoid pursuing enforcement under CIRCIA or allowing CIRCIA reports to be the basis for enforcement actions by other Federal agencies under separate regulations. Security measures to protect reported information must also be robust to ensure all data reported is protected from unauthorized access and breaches.

Costs:

Many APTA members are facing operating budget shortfalls, also known as the "fiscal cliff." In an APTA survey conducted in May of 2023, one-half of responding agencies stated they are facing a fiscal cliff in the next five years. Many of these agencies will fall under this regulation and may not have the capability or resources to respond operationally to a significant cyber incident, or to follow required reporting procedures within the specified timeframe. Such requirements may prove to be extremely burdensome on smaller agencies due to the sheer lack of resources and trained cybersecurity professionals at their disposal, placing them at risk of noncompliance and unjustly on the receiving end of the outlined enforcement protocols.

APTA encourages an increase in grant funding to transit agencies to ensure that they have the resources to meet minimal established cybersecurity standards.

Definitions:

CISA should provide a more precise definition of "substantial cyber incidents." Detailed examples of industry specific incidents would be helpful.

Information Exchange:

APTA recommends CISA implement structured threat information expression (STIX) and trusted automated exchange of intelligence information (TAXII) for the quick dissemination of reported indicators of compromise (IOCs) back to stakeholders and integrate reported intelligence into accessible large language models (LLMs).

APTA members would like CISA to make anonymized/abbreviated cyber incident report information available through the Public Transportation Information Sharing and Analysis Center (PT-ISAC) and other forums so that industry can see the types of incidents reported to ensure that they have appropriate threat mitigation measures in place.

Supplemental Report:

APTA supports CISA's proposal to allow covered entities to submit new or updated information in a supplemental report as additional information becomes known about the covered cyber incident. APTA recommends the reporting method used for the original incident report also be used for supplemental reports.

Information Protection:

APTA members expressed concern about the potential of an inadvertent release of data associated with cyber incident reports through a data breach or other incident. There is substantial risk associated with CISA's collection and retention of detailed information on the cyber defenses and vulnerabilities for all critical infrastructure entities that experience cyber incidents.

.

CISA should take steps to ensure the confidentiality of the information, including the identity of the victims of a reported cyber incident included in CIRCIA reports. CISA should also anonymize and aggregate cyber incident report information prior to sharing it with others. CIRCIA reports and/or the information contained therein should be exempted from release under the Freedom of Information Act and similar state laws. APTA members recommend that information reported to CISA in CIRCIA reports be handled as Protected Critical Infrastructure Information and afforded those protections.

Summary:

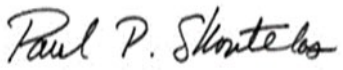
In summary, APTA appreciates this opportunity to provide comments on the Cyber Incident Reporting for Critical Infrastructure Act of 2022 NPRM.

Safety is the number one core value of APTA, and our members. APTA continues to advance cybersecurity through a website resource page, webinars, conference sessions, the development of standards and an eLearning course. APTA has advocated that transit agencies integrate their cyber risk management programs into an enterprise risk management program.

APTA strongly encourages CISA to coordinate with TSA throughout the rulemaking process to harmonize CIRCIA's applicability with the TSA security directives and other future rulemaking. We look forward to continuing to work with CISA to improve cybersecurity throughout the transit industry.

If you have any questions regarding this letter, please contact Polly Hanson, APTA's Senior Director of Security, Risk and Emergency Management, at phanson@apta.com or 202.496.4895.

Sincerely,



Paul P. Skoutelas
President and CEO