STATEMENT OF

IAN JEFFERIES

PRESIDENT AND CHIEF EXECUTIVE OFFICER

ASSOCIATION OF AMERICAN RAILROADS

BEFORE THE
U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON HOMELAND SECURITY

SUBCOMMITTEE ON TRANSPORTATION
AND MARITIME SECURITY

HEARING ON
IMPACTS OF EMERGENCY AUTHORITY CYBERSECURITY REGULATIONS ON THE TRANSPORTATION SECTOR

NOVEMBER 19, 2024

Association of American Railroads
425 Third Street SW
Washington, DC 20024
202-639-2100

Introduction

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to testify on how the rail industry works with our government counterparts to address cyber threats and the impacts of emergency authority on those efforts. AAR's members account for the vast majority of North American freight railroad mileage, employees, and traffic.

Freight railroads integrate skilled personnel and ingenuity with technology to keep the network infrastructure safe and the supply chain moving every day. Advanced information and communications technology are helping our employees in every aspect of our operations, including train control, track and equipment inspections, emergency response, dispatching, railcar tracking, locomotive fuel management, predictive performance analysis, employee training, and much more. Cybersecurity is an arms race between attackers and defenders, which is why our highly skilled, highly trained employees work diligently to continually enhance their capabilities and guard against cyberattacks that threaten the safety and integrity of our operations.

For 25 years, railroads have maintained a dedicated coordinating committee focused on cyber threats, effective risk mitigation practices, and engagement with appropriate government entities. Railroads leverage a strong mix of private and public capabilities to effectively prevent and respond to malicious cyber activity. As threats evolve, our industry strives to stay agile and innovative to address the dynamic threat landscape.

A Unified Commitment to Overall Security Preparedness

The rail industry addresses cybersecurity head on through a longstanding industry-wide, risk-based, and intelligence-driven plan. Railroads' highly specialized cybersecurity teams carry

out comprehensive, multi-faceted cybersecurity plans focused on four factors identified by experts as the most likely way to stop cyberattacks: the tactics most commonly used to gain illicit access to computer systems; the vulnerabilities most commonly exploited; illicit activities missed or disregarded in prior analysis but identified after the incident; and protective measures that could have made a difference had they been implemented.

Responsibility for implementing and sustaining cybersecurity plans lies with two specialized industry coordinating bodies. First, the Rail Security Working Committee includes senior law enforcement and security officials focused on countering domestic and international terrorism. Second, the Rail Information Security Committee (RISC) is comprised of chief information security officers and information assurance leaders from major North American railroads. The RISC was established in 1999 and is supported by security experts from the AAR and the American Short Line and Regional Railroad Association (ASLRRA). Together, these committees form the Rail Sector Coordinating Council (RSCC), the rail industry's primary channel for communication and coordination with government agencies on cybersecurity initiatives.

The rail industry's security plan does not just sit on a shelf. It is a living document, continuously evaluated and enhanced through recurring exercises and frequent consultations with government and private-sector security experts to ensure maximum sustained effectiveness supported by a strong working relationship with the federal government.

Information Sharing is Vital for Success

For railroads, cyber awareness is a fundamental component of their day-to-day operations, but even the best cybersecurity plans and practices will falter if useful information on cyber threats is not shared. Information sharing allows organizations to learn from one another,

reduce their vulnerabilities, and quickly adapt to changing conditions. Insights gained from risk assessments and threat advisories, along with experience gained in drills, enable railroads and industry organizations to incorporate effective safeguards and protective measures into their own systems.

For this reason, railroads and industry organizations prioritize proactive engagement with government partners, including the Transportation Security Administration (TSA) and the Cybersecurity and Infrastructure Security Agency (CISA), to share information on cyber threats and effective countermeasures. These open lines of communication are maintained through frequent calls and meetings between AAR, its members, and TSA, ensuring our federal government partners are aware of how rail operations interact with cybersecurity measures.

Noticed of Proposed Rulemaking (NPRM)

Earlier this month, TSA issued a lengthy NPRM that builds upon existing cybersecurity requirements previously issued through security directives. While the industry was pleased to see TSA issue this rule through the regulatory process and allow for robust public comment, the NPRM would have greatly benefited from earlier discussions with industry about potential requirements in a more informal setting like negotiated rulemaking. The industry is still digesting the very lengthy proposal and will provide robust comments. There are a few long-standing concerns for the railroads that the NPRM does not fully address.

For example, the NPRM would require railroads to report an incident within 24 hours of it occurring. Congress specifically set the timeframe for reporting incidents at 72 hours under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA). Not only does this lack of harmonization create confusion, the 24-hour window is impractical. Within 24 hours, an attack could still be occurring, the information about the incident will be less complete, if not

inaccurate, and railroads would be pulling resources and manpower away from responding to the attack and towards complying with reporting requirements. The railroads would have to then supplement the initial report as their information becomes available or changes.

Similarly, the NPRM also requires that a railroad's security coordinator be a U.S. citizen, which the railroads have flagged with TSA as a major concern for several years. Two large railroads in the U.S. are headquartered in Canada and employ Canadian citizens in high-level cybersecurity roles. Prohibiting these highly skilled senior level employees from representing their companies as security coordinators serves no clear security benefit and makes it extremely difficult for these Canadian railroads to comply.

Use of TSA Emergency Authority

AAR was pleased that TSA finally issued this NPRM. For several years, the industry was operating under security directives issued under TSA's emergency authority. We recognize the importance of TSA having the appropriate authority to act quickly in the face of an emergency. However, following the Colonial Pipeline attack in 2021, TSA used its emergency authority to issue security directives aimed at freight railroads and other modes of critical infrastructure mandating specific requirements effective immediately. AAR was unaware of, nor was it made aware of, any prevailing freight rail emergency conditions that would require use of emergency authority, and the security directives circumvented the notice and comment period that allows for industry feedback to improve regulations. The broad mandates TSA issued also treated every mode as if they were starting from scratch with developing a cybersecurity plan when railroads had been properly monitoring their network for decades. The decision by TSA to issue the recent NPRM and move away from security directives and towards the normal rulemaking process is a welcome one that will make these regulations more effective.

Other Areas for Improvement

AAR has identified two other areas where our work with TSA and other agencies could be improved. First, the lack of analysis of cyber incidents by the government can leave railroads and other modes unaware of future threats or how to reduce susceptibility to future attacks. Further analysis of an attack or other incidents by the government can inform railroads' decisions about strengthening our network. Second, the government's focus on the cybersecurity risks of transportation companies overlooks the importance of ensuring the security of suppliers to the industry. Suppliers play a critical role in various aspects of railroad operations, and the government should consider how best to directly address their vulnerability to cyber incidents.

Conclusion

The railroad industry, TSA, and CISA share a common purpose: ensuring that effective, up-to-date, and sustainable measures are in place to mitigate risk in the face of evolving cyber threats. Railroads have a proven track record of cooperative engagement with federal agencies, and they firmly believe that collaborative effort is the best way to achieve this goal. Railroad operations are resilient thanks to years of proactive and extensive efforts by highly skilled railroad employees to develop, implement, and continuously improve plans, practices, and measures for cybersecurity as threats and security concerns emerge. Cybersecurity is always evolving, and real-time adaptation is essential to reduce risk. Railroads and their employees will continue to work cooperatively with private and public entities to ensure that our nation's rail network and the people, firms, and communities we serve remain safe, efficient, and secure.