STATEMENT OF

THOMAS FARMER

ASSISTANT VICE PRESIDENT - SECURITY

ASSOCIATION OF AMERICAN RAILROADS

BEFORE THE
U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

HEARING ON "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure"

NOVEMBER 4, 2021

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

On behalf of the members of the Association of American Railroads (AAR), thank you for the opportunity to offer this testimony. AAR's freight railroad members account for the vast majority of North American freight railroad mileage, employees, and traffic. Passenger railroad members include Amtrak and several major commuter carriers as well.

Railroads are indispensable to our nation. They connect producers and consumers of goods across the country and the world, expanding existing markets and opening new ones. Whenever Americans grow something, mine something, or make something; when they send goods overseas or import them from abroad; when they eat their meals or take a drive in the country, there's an excellent chance freight railroads helped make it possible. Passenger railroads enhance mobility and connectivity, alleviate highway and airport congestion, reduce pollution, promote local and regional economic development, and improve transportation safety.

Unified Commitment to Security Preparedness, and Continuous Improvement

Railroads and rail industry organizations address both cyber and physical security through unified efforts under a longstanding comprehensive security plan. Applying a risk-based and intelligence-driven approach to rail security, this plan has four alert levels that call for increasingly stringent security measures.

Responsibility for managing the security plan and assuring its sustained effectiveness to meet evolving threats is vested in two dedicated industry coordinating committees: the Rail Security Working Committee, which is comprised of senior law enforcement and security officials focused on domestic and international terrorism; and the Rail Information Security Committee (RISC), which consists of the chief information security officers and information assurance officials of major North American railroads, with support from security experts at AAR and the American Short Line and Regional Railroad Association (ASLRRA). The rail industry, through RISC, has maintained a dedicated and effective coordinating forum for cybersecurity protection and risk mitigation for more than two decades. Together, the two committees constitute the Rail Sector Coordinating Council (RSCC), which serves as the rail industry's main channel of communication and coordination with government agencies on cyber and physical security and preparedness.

Because of the devoted work of these committees, the rail industry's security plan does not just sit on a shelf, occasionally taken down and dusted off. Rather, it is a living document, evaluated and enhanced continuously through recurring exercises, integration of effective practices, and frequent consultations with government and private-sector security experts to ensure maximum sustained effectiveness in the face of evolving security threats. Early in 2020, the two industry committees completed the most substantial review and update of the plan since its inception some 20 years ago. This update highlighted the substantial progress the industry has made in terms of capabilities, monitoring and analysis of threats, coordination with government agencies, electronic reporting, and joint decision-making on alert levels, measures, and actions.

Railroads Address Cybersecurity Head On

Railroads of all kinds rely on advanced software and information technology in every aspect of their operations. These technologies run the gamut from advanced train dispatching software to smart sensors along tracks that identify equipment in need of repairs, and from real-time shipment tracking tools to sophisticated train control technology.

Railroads recognize their critical importance to our nation, as well as the risks associated with their extensive reliance on information technology, which is why they are continuously on guard against cyberattacks and working diligently to enhance their capabilities to guard against them. Railroads' cybersecurity efforts are comprehensive, multi-faceted, and supported by specialized, highly skilled cybersecurity staff.

A recent report by the Congressional Research Service rightly concludes, "Cybersecurity is a risk management process rather than an end-state. It involves continuous work to (1) identify and (2) protect against potential cybersecurity incidents; and to (3) detect; (4) respond to; and (5) recover from actual cybersecurity incidents." Entities "may choose to evaluate their information technology (IT) risks by understanding the threats they are susceptible to, the vulnerabilities they have, and the consequences a successful attack might have for their mission and their customers."[1] The rail industry consistently focuses on these priorities through unified, multifaceted, and proactive cybersecurity efforts.

Rail Industry Cybersecurity Efforts Span Two Decades

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. For this reason, railroads and industry organizations prioritize proactive engagement with government partners to share information on cyber threats and effective countermeasures. 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.

[1] Congressional Research Service, "Federal Cybersecurity: Background and Issues for Congress," September 29, 2021. Available at https://crsreports.congress.gov/product/pdf/R/R46926.

The rail industry focuses on analyzing four categories of protective measures: the tactics most commonly employed to gain illicit access to computer systems; vulnerabilities most commonly exploited; indicators of illicit activities most often noted in post-incident analyses that were missed or disregarded; and protective measures that could have made a difference if they had been implemented. We use these four categories based on experience best demonstrated by the Australian Cyber Emergency Response Team (CERT), which found that the vast majority of the cyberattacks against private entities in which CERT provided aid would not have been successful if the targeted entity had paid sufficient attention to these four protective measures.

Further steps that the rail industry has taken to enhance timely information sharing, in coordination with partners at DHS, FBI, TSA, and DOT, include:

- Deploying secure telephone equipment to connect major railroads, the AAR, and government officials.
- Sharing classified information with authorized Canadian railroad officials who hold security clearances issued by the government of Canada.
- Establishing a classified information sharing network with TSA, which enables authorized rail industry personnel to review relevant materials in dozens of metropolitan areas nationwide.
- Participating in a multi-industry initiative with DHS to establish a secure video teleconference network that simultaneously links more than 40 U.S. metropolitan areas.

As a result of these cooperative efforts between industry and government, what had often required weeks, or even months, of effort can often now be accomplished in hours. This progress greatly enhances the ability of those in the private and public sector to identify and effectively respond to cyberthreats in a collaborative manner.

The President Urges Government-Industry Collaboration on Cybersecurity

The rail industry supports the President's emphasis on government-industry collaboration to enhance cybersecurity as laid out in the National Security Memorandum on *Improving Cybersecurity for Critical Infrastructure Control Systems*, issued on July 28, 2021.

In response to the memorandum, the rail industry developed a detailed proposal on how government and industry can work collaboratively to elevate cybersecurity posture in all transportation modes. We submitted this to TSA just three weeks after the memorandum was issued and more than a month before TSA's initial outreach to stakeholders regarding Security Directives to mandate cybersecurity measures by railroads and rail transit agencies.

Work on this initiative began over two months earlier in the wake of the Colonial Pipeline cyberattack. In early June 2021, AAR's security lead joined his colleague at the American Public Transportation Association (APTA) to propose a "strategic concept" for enhancing cybersecurity in the transportation sector. Over the next couple of months, the rail industry took the lead in drafting this strategic concept.

Submitted in mid-August, the industry proposal delineates 13 areas of emphasis that outline actions for transportation organizations and federal government organizations to take to implement TSA's Cybersecurity Roadmap. TSA Administrator David Pekoske has frequently cited the Roadmap as defining "clear pathways" for enhancing cybersecurity posture and mitigating cyber risk in the transportation sector. Additionally, the rail industry's August proposal covers recommend conduct of cybersecurity self-assessments, something on which TSA plans to issue a non-compulsory information circular.

Unfortunately, although the rail industry's strategic concept proposal was submitted in August and meets the President's repeated emphasis on collaboration to enhance critical infrastructure cybersecurity, we have received no official response.

TSA Security Directives Are Unnecessary

As members of this committee know, in public remarks about a month ago, Secretary of Homeland Security Alejandro Mayorkas announced that TSA will issue Security Directives laying out cybersecurity actions and measures that must be implemented by "higher-risk railroad and rail transit entities." In making this announcement, Secretary Mayorkas said, "There is no better example of how the cybersecurity threat can impact our lives than in the transportation sector and how people commute, see one another, engage with one another."

Railroads and industry organizations certainly agree that the cybersecurity threat merits priority attention – as demonstrated by the rail industry's rigorous attention to this issue for more than 20 years. Significantly, each of the actions the Secretary said will be covered by TSA security directives for railroads and rail transit agencies is already covered by the rail industry's August 2021 proposal noted above. Put another way, railroads are already doing what they should be doing in terms of cybersecurity.

Moreover, issuing a Security Directive is an exercise of emergency authority by the TSA Administrator that allows imposition of requirements "immediately in order to protect transportation security."[2] Railroads and rail industry organizations have not been advised by federal officials of any prevailing emergency conditions that justify use of this authority, despite the many opportunities available. TSA officials have indicated that work to produce and provide

[2] 49 U.S.C. § 114(l).

a current cyber threat briefing is ongoing, but to our knowledge no briefing has been proposed or scheduled for this purpose.

In addition, the Security Directives could undermine the 20-year effort of the industry to develop and share cybersecurity information among railroads and government agencies, as explained above. If reports are required to be made to government and are deemed security-sensitive information, then private industry stakeholders may be reluctant to share the information through our established network. This outcome will ultimately have a deleterious effect on the security of the industry and the purported goal of these proposed Security Directives.

Lastly, the announcement of the Security Directives has produced erroneous perceptions that railroads, and rail transit agencies, have not been rigorously and effectively engaged for many years in defending against cyber threats. This false impression could have negative ripple effects if rail customers and the communities in which railroads operate lose confidence in railroads' ability to operate safely and securely.

Railroads' cybersecurity efforts are far more likely to be effective if they involve continued collaborative efforts with government than if they are mandated through top-down security directives or rulemakings. To that end, our concerns are as follows:

- The requirement that the appointed primary and alternate cybersecurity coordinators be U.S. citizens will make compliance by two major Canadian railroads (CN and Canadian Pacific) that also have substantial U.S. operations extremely difficult. Given that TSA and the rail industry have long successfully shared classified information with Canadian nationals who hold security clearances issued by the government of Canada, this prescriptive measure is unwarranted.
- The mandate to report a "cybersecurity incident" is overly broad and, if left unchanged, will result in high volumes of reports on matters that are not significant from a

cybersecurity perspective. The directive should focus instead on "significant" cybersecurity incidents so that developing threats and effective preventive measures can be more readily identified.

- The inflexibility of an overriding government mandate of risk-based determinations on preparedness and response planning, protective measures, and implementing capabilities.

What Future Cybersecurity Legislation Should Include

As noted above, information sharing is crucial to the success of all cybersecurity plans. The Cybersecurity Information Sharing Act of 2015 (CISA 2015) expressly authorized sharing of cyber threat intelligence and related security information and created a framework of protection to facilitate and encourage such exchanges within industries, across critical infrastructure sectors, and with federal government entities. Unfortunately, many of the authorizations and protections Congress established in CISA 2015 have either been inconsistently utilized or left unimplemented.

Policymakers should build upon the collaborative approach described in this testimony and that has worked effectively for years, rather than implementing mandates that would needlessly disrupt existing organizational structures and practices that prove their value daily. In this regard, freight railroads respectfully suggest that the following elements should be included in future cybersecurity legislation:

1. Include the reasonable protections provided in CISA 2015.

- ✓ Antitrust exemptions, civil liability protections, and other protections (Division N—CISA 2015; Secs. 104(e), 105(d));
- ✓ Disclosure law exemptions, such as freedom of information statutes, open meetings laws, or similar enactments requiring the disclosure of information or records at the

state, federal, and tribal or territorial levels (Division N—CISA 2015; Sec. 104(d)(4)(B)(ii)); and

- ✓ Certain regulatory use exemptions, which prevent any federal, state, tribal, or territorial government from bringing an enforcement action based on the sharing, but not the development or implementation, of a regulation (Division N—CISA 2015; Sec. 104(d)(4)(C)(ii)).

Together, these provisions provide reporting entities with the protections and confidence needed to sustain the unencumbered flow of cybersecurity information with government authorities. Including these protections in all future cybersecurity legislation will build upon the successful partnerships CISA 2015 has formed.

2. Expand the analytical capabilities of the Cybersecurity and Infrastructure Security Agency's (CISA) workforce.

Private sector entities, including railroads, already report significant cybersecurity incidents and security concerns to CISA and other federal government agencies. A persistent challenge, raised often by private sector entities with federal partners, is the lack of analysis of the reports by the government. Given the breadth of the reporting mandate in the planned Security Directives for railroads and rail transit agencies, the volume of reporting to CISA will increase substantially. CISA must have the capacity to review, evaluate, and analyze reports received from railroads and rail transit agencies. Feedback should focus on why the reported activity matters to those transportation organizations and what can be pragmatically done in order to narrow future susceptibility. The lack of this focused analysis and feedback to transportation sector entities indicates that CISA may lack staffing and resources to meet this need.

3. Direct CISA to regularly update a cyber threat profile based on analyses of attacks, failed attempts, and successful disruptions.

This profile should focus on the following parameters:

- Tactics most commonly used to perpetrate breaches;
- Vulnerabilities most frequently targeted and exploited;
- Protective measures most often found lacking or inadequately implemented that could have prevented incidents; and
- Indicators of developing threats that are often missed or misunderstood.

The aim is to build understanding of how prevailing cyber threats materialize and the measures most effective to prevent them or seriously mitigate their adverse effects. The profile should undergo constant review to enable updates on a quarterly basis. Organizations across sectors and industries would contribute to the development of this profile through reporting on significant cyber threats, incidents, and indicators of concern and on measures or actions taken for risk mitigation.

4. Direct CISA and Sector Risk Management Agencies (SRMAs) to work with private entities to establish early notification networks.

The importance of cyber-attack analyses rests in what they yield, which are discernible indicators that assist in identifying the illicit activity that took place. Consistency in identifying and sharing these indicators in a timely and efficient manner is crucial to prevent and mitigate future attacks. Early notification networks provide an effective means for proactive, streamlined, and continuous sharing by governmental and private entities of these types of indicators based on trust and shared interests.

5. Define and publicize procedures for stakeholders to submit requests for information (RFIs) and requests for assistance (RFAs) to enhance cooperative cybersecurity efforts.

As part of cyber preparedness plans, as well as in the wake of a cyber-attack that affects a particular entity or industries, organizations across sectors use RFIs and RFAs to gain insights based on federal analyses of cyber threats and risk mitigation measures. Timely responses can make prevention attainable. Unfortunately, CISA, Sector Risk Management Agencies (SRMAs), and other federal components lack consistency regarding submission, review and consideration, and responses to RFIs, RFAs, and proposals for action to enhance cybersecurity. Ad hoc processes are applied. These can vary substantially with the type of incident, the information or action sought, and the federal government organization that takes responsibility for acting on the request or proposal. The result is a lack of response or an action that fails to meet the stated needs or reasonable expectations.

6. Direct CISA to establish consistent standards for software bills of materials (SBOM) from vendors and suppliers

A recurring theme in the evaluation by CISA of cyber-attack campaigns over the past year is the exploitation of vulnerabilities in software that end users could not detect. To redress this gap in cybersecurity awareness, CISA has repeatedly urged end users to ask their suppliers to provide a software bill of materials that provides an inventory list of all open source/third-party components present in the source code used to build a particular software system, application, or software or component. Legislation should transition CISA's recommended measure and define consistent and effective practices for vendors and suppliers of information technology. Proven supported equipment, devices, and components need to produce sturdy software bills of materials and make them available or accessible to their buyers and end users.

The railroad industry, TSA, and CISA share a common purpose: ensuring that effective and sustainable measures are in place, and regularly reviewed for continuous improvement, to mitigate risk in the face of evolving cyber threats. Railroads have a proven track record of cooperative engagement with federal agencies, and we firmly believe that collaborative effort is the best way to achieve this aim. We should be afforded the opportunity to do what the President so rightly urges in his National Security Memorandum.

Thank you again for the opportunity to present this testimony. When it comes to cybersecurity, railroads have been proactive, effective, and collaborative for many years. They will continue to work cooperatively with private and public entities to ensure that our nation’s rail network and the people, firms, and communities it serves, remain protected.