Freight Rail & Cybersecurity Legislation

**Freight Rail Policy Position:** Freight rail emphasizes the importance of cyber resiliency and maintaining public trust as critical infrastructure. Cybersecurity legislation should enable nimble and effective response capabilities without liability concerns, and direct relevant agencies to establish consistent procedures for timely government analysis and support.

Railroad logistics are 24/7, and cyber network protection is no different. By tapping into the full range of private and public capabilities, freight railroads ensure effective preparedness, prevention and response to mitigate the effects of cyber-attacks.

Railroads maintain a dedicated cybersecurity committee that has functioned for more than 20 years. Railroads also continuously collaborate and share information with federal government agencies like the Department of Homeland Security (DHS), Transportation Security Administration (TSA), Federal Bureau of Investigation (FBI), Department of Transportation (DOT), and Department of Defense (DoD) commands and components. Freight railroads recognize that cyber resiliency is a must, as is maintaining the public’s trust as a proactive critical infrastructure organization. Below are freight rail’s recommendations.

1. **Ensure CISA 2015 protections are implemented in all future cyber legislation.**

A key part of the Cybersecurity Information Sharing Act of 2015 (CISA 2015’s) importance and impact is the statute’s proper protection for private entities reporting on cybersecurity. The protections include: Antitrust exemptions and civil liability protections (Division N—CISA 2015; Sec. 104(e)); 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 that 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)(i)).

Together, these provisions provide reporting agencies the protection and confidence needed to enable and sustain the unencumbered flow of cybersecurity information between reporting entities and the federal government. Including these protections in all future cybersecurity legislation will build upon the successful legacy and partnerships CISA 2015 has formed.
2. Expand the CISA workforce’s analytical capabilities.

The Cybersecurity and Infrastructure Security Agency (CISA) must be authorized to increase the technical understanding of its workforce before requiring more cybersecurity reporting. Private entities recognize the challenging role that CISA plays by maintaining broad perspectives across critical infrastructure sectors, departments and federal agencies. This unique position should create a substantial opportunity to identify and respond to threats from various sources that impact public and private entities.

Yet, a persistent concern remains. Having been raised repeatedly with CISA, TSA, DOT, and DoD, there is a severe lack of analysis received in follow-up reports submitted regarding illicit cyber activity. This analysis should produce security alerts that highlight trends, patterns, and indicators of concern, but they consistently fall short. As a result, private entities have reported a lack of effective action by CISA on submitted reports. This continuing gap indicates that CISA, as currently staffed, is not equipped with the appropriate personnel to perform the type of analysis and response needed to ensure the most effective cybersecurity incident prevention and response.

Without a simultaneous increase in threat assessment, broadly defined mandates for cyber incident reporting will not improve our nation’s cybersecurity. Instead, the undesired effect will overload CISA’s already burdened analytical capability with high reporting volumes — most of which are on insignificant cyber activity.

3. Direct CISA to regularly update a cyber threat profile based on key data.

To understand how cyber threats manifest and the measures most effective in preventing or mitigating their effects, it is important to realize two critical truths of cybersecurity. First, what happens worldwide affects us here at home; thus, lessons are continuously being applied to elevate our cybersecurity posture.

Second, when creating standard operating procedures, less is more. A clear and concise cyber threat profile would highlight how cyberattacks occur, why they succeed and what actions are most effective for prevention. Entities across sectors would use this profile to maintain informed vigilance, elevate cybersecurity posture in sustainable ways and mitigate risk exposure.

Example: Analyses by the Australian Cyber Emergency Response Team had determined that in 85% of the cyber-attacks that affected private sector entities in Australia, the adverse impacts could have been prevented if these four categories of protective measures had been implemented and sustained: Tactics most commonly used to perpetrate breaches; Vulnerabilities most frequently targeted and exploited; Indicators of developing threats that are often missed or misunderstood; and inadequately implemented protective measures that could have prevented incidents. A similar outcome is attainable in the United States, and given its success, CISA should closely review this model and provide guidance for procedures that are equally as clear, concise and effective.
4. Direct CISA and SRMAs to create early notification networks with private entities.

After every cyber-attack, a traceable event known as an indicator of compromise occurs. However, identifying these indicators rests solely on the quality of post-attack analysis, only further emphasizing the expediency and sharing of these indicators amongst known stakeholders. Early notification networks provide these indicators of compromise to federal government security operation centers and back to private entities. These early notification networks also create patterns and timely responses to developing threats.

Private entities have recognized early notification networks as a necessity for streamlined reporting. However, the federal government does not have an early notification network as robust as private entities. While steps are being taken to reconcile this through like-technology implementations, much work remains and should be encouraged. Cybersecurity legislation should reinforce and build upon the authorizations and protections accorded by the CISA 2015 to define the parameters for early notification networks jointly managed by Sector Risk Management Agencies (SRMAs) and the critical infrastructure Sector Coordinating Councils with which they work.

5. Use RFIs and RFAs to enhance cooperative cybersecurity efforts.

The Federal government has the impressive ability to access and compile data across a swath of public and private entities; however, its ability to analyze that data efficiently and adequately is lacking. That is where requests for information (RFIs) and requests for assistance (RFAs) come in. As part of cybersecurity preparedness, RFIs and RFAs are used to gain insights based on federal analyses of cyber threats by drawing on the unique perspective that government cybersecurity analysts attain based on patterns, trends and indicators of significant cybersecurity concern.

Unfortunately, consistency in practice and procedures lacks action by CISA, SRMAs, and other federal components on procedures for submission, review and consideration, and response for RFIs and RFAs. If an attack on critical infrastructure happens in Israel, for example, an established standard operating procedure surrounding RFIs and RFAs will increase the capabilities of domestic private entities. Cybersecurity legislation should direct CISA and SRMAs to define and publicize consistent procedures that prompt timely action regarding government analysis and support for RFIs and RFAs.

Trains interchanged at the southern border were previously required to come to a complete stop on the single-track Laredo International Rail Bridge to change crews, a process that could take over an hour. The process has sometimes made the border a bottleneck, resulting in security and public safety risks as 125 standing rail cars — vulnerable to theft, vandalism and trespassing — block multiple streets and highway crossings on both sides of the border.