Published on *The National Law Review* https://natlawreview.com

TSA Announces Proposed Pipeline, Railroad, Bus Cybersecurity Rules

Article By:

Hunton Andrews Kurth’s Privacy and Cybersecurity

On November 6, 2024, the Transportation Security Administration (“TSA”) published a Notice of Proposed Rulemaking (“NPRM”) that would subject critical surface transportation owners and operators to cyber risk management and reporting requirements. The NPRM, which is titled Enhancing Surface Cyber Risk Management, contains rules that would apply to certain pipeline and rail owners and operators, with some bus operators subject to less prescriptive requirements.

The proposed rules build on the security directives the TSA has issued since 2021 to require owners and operators of certain critical pipeline and railroad systems to implement specific cybersecurity measures. The security directives, as well as the new proposed rules, are part of the TSA's strategy intended to strengthen the cybersecurity posture of the U.S.'s critical infrastructure following a high-profile ransomware attack on a major U.S. pipeline in 2021.

The proposed rules would require owners and operations of designated railroad and pipeline systems and facilities to establish a cyber risk management (“CRM”) program approved by the TSA. The CRM program would need to include the following three primary elements.

- **Conduct annual cybersecurity evaluations**
  Covered entities would be required to annually perform an enterprise-wide cybersecurity evaluation that evaluates the entity's cybersecurity profile compared to a target profile.
- **Prepare a Cybersecurity Operational Implementation Plan (“COIP”)**
  Covered entities would also be required to develop a TSA-approved COIP. The COIP would include information such as (1) a list of individuals responsible for the CRM, including an accountable executive and a cybersecurity coordinator; (2) a description of the entity's critical cyber systems, network architecture issues and baseline communications; and (3) details about the measures taken to protect critical cyber systems, detect cybersecurity incidents and address post-incident remediation efforts.
- **Develop a Cybersecurity Assessment Plan (“CAP”) to identify unaddressed vulnerabilities**
  The proposed rule would require covered entities to prepare a CAP that identifies unaddressed security vulnerabilities, outlines a plan to assess the effectiveness of the COIP, includes a schedule for security assessments and provides for the annual reporting of assessment results.

In addition to the CRM requirements, the proposed rules would create a distinction between physical security and cybersecurity reporting requirements. Under the proposed rules, owners and operations would have to report significant physical security concerns to TSA and report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (“CISA”). In line with this proposal, the proposed rules would mandate owners and operators of designated pipeline facilities to report both physical security and cybersecurity incidents.

Finally, the proposed rules would harmonize the TSA's process of issuing pipeline and rail-specific security directives with the procedures currently applicable to the aviation industry, creating a consistent approach for all modes of transportation regulated by the agency.

The TSA requests comments on the proposed rules by February 5, 2024.

National Law Review, Volume XIV, Number 339

Source URL:https://natlawreview.com/article/tsa-announces-proposed-pipeline-railroad-bus-cybersecurity-rules