Van Ness Feldman LLP
vnf.com

TSA Requests Input from Pipeline and Rail Sectors on Cyber Risk Management to Inform New Regulations

DECEMBER 5, 2022

Nakia Arrington, Michael Diamond, and Susan Olenchuk

On November 30, 2022, the Transportation Security Administration ("TSA") issued an advanced notice of proposed rulemaking ("ANPRM") announcing that the agency intends to issue regulations governing cyber risk management ("CRM") in the pipeline and rail industries and seeking input from industry stakeholders to inform the new regulations. The ANPRM requests that stakeholders respond to dozens of questions regarding their current and planned CRM practices in order to inform TSA's efforts to enhance pipeline and rail cybersecurity. The ANPRM is TSA's first step towards the possible adoption of new regulations to govern CRM practices in these sectors.

Comments on the ANPRM are due January 17, 2023.

Background

The ANPRM describes "cyber risk management" as "all activities designed to identify and mitigate risk-exposures to cyber technology, both informational and operational, to ensure safe, sustained operations of vital systems and associated infrastructure." While TSA conducts physical security assessments of certain pipelines and has adopted regulations addressing security training for the rail industry, TSA has not adopted regulations addressing the CRM practices of these sectors. To date, TSA has addressed cybersecurity in these industries by encouraging voluntary implementation of recommended guidelines and through mandatory security directives issued to higher risk pipeline and rail facilities in 2021 and 2022.

TSA has determined that the issuing of CRM regulations is necessary given the critical role of the pipeline and rail industries to the nation's economy and national security, as well as the persistent and growing cyberthreats to these industries. Pursuant to its general statutory authority to protect transportation security and the Implementing Recommendations of the 9/11 Commission Act of 2007, TSA has issued the ANPRM to initiate a rulemaking process to address CRM practices of the pipeline and rail sectors.

TSA's Policy Priorities

The ANPRM identifies the following seven policy priorities that will guide TSA's rulemaking initiative: (1) assessing and improving the current baseline of operational resilience and incident response; (2) maximizing the ability for owner/operators to be self-adaptive to meet evolving threats and technologies; (3) identifying opportunities for third-party experts to support compliance; (4) accounting for the differentiated cybersecurity maturity across the surface sector and regulated owner/operators; (5) incentivizing cybersecurity adoption and compliance; (6) measurable outcomes; and (7) regulatory harmonization.

TSA also identifies the following core elements that the agency believes will provide "a bedrock" of CRM for the pipeline and rail sectors: the designation of an individual responsible for cybersecurity; access controls; vulnerability assessments; measures to evaluate the implementation, effectiveness, efficiency, and impact of cybersecurity controls; drills and exercises; technical and physical security controls; incident response plan and operational resilience; incident reporting and information sharing; personnel training and awareness; supply chain and third-party risk management; and recordkeeping and documentation. TSA also is interested in understanding cost implications.

Request for Specific Comments

To help it understand how the pipeline and rail sectors are currently implementing CRM and to aid it in developing a thorough and well-researched rulemaking that addresses forward-looking challenges, TSA asks a variety of questions that are categorized under six general topics. TSA states that these questions are not all-inclusive and welcomes supplemental information.

1. **Identifying Current Baseline of Operational Resilience and Incident Response**. TSA asks about operators' current cybersecurity measures, and measures planned for the near future. This includes questions about whether operators use objective standards to assess their preparedness, and costs and benefits of using such standards.

2. **Identifying How CRM Is Implemented.** TSA asks operators to describe how they have implemented CRM practices and how they are planning to do so. This includes questions on the costs of CRM practices, the availability of third-party contractors to assist with these matters, and internal training requirements.

3. **Maximizing the Ability for Owner/Operators to Meet Evolving Threats and Technologies.** TSA asks numerous questions pertaining to the appropriate scope of regulation. It asks what types of cyber systems TSA regulations should address and how regulations can keep up with the continually evolving nature of cyber threats. It also asks about the impact cybersecurity regulations could have on operations, and for recommendations concerning the design of the regulations.

4. **Identifying Opportunities for Third-Party Experts to Support Compliance**. TSA asks questions about the role of third parties in establishing compliance with regulations, such as through verifications and validations. This includes questions regarding how such entities could be used, and benefits and challenges related to any required third-party accreditations.

5. **Cybersecurity Maturity Considerations**. TSA asks about special considerations pipeline and rail sectors would need to consider before implementing CRM practices, such as costs, risks, and practical limitations. It also considers that operators could be subject to cybersecurity regulations from multiple agencies and seeks suggestions on how to achieve regulatory harmonization.

6. **Incentivizing Cybersecurity Adoption and Compliance**. TSA asks what types of measures could be used to incentivize compliance, including liability protection, insurance, commercial contracts, or other private or public sector options.

For More Information

Van Ness Feldman can assist in analyzing and commenting on the ANPRM and potential future regulations for the pipeline and rail sectors. Please contact Susan Olenchuk, Michael Diamond, Nakia Arrington, or any other member of the Pipeline & LNG Practice Group or Cybersecurity and Emerging Technologies Team.

Follow us on Twitter @VanNessFeldman

This document has been prepared by Van Ness Feldman for informational purposes only and is not a legal opinion, does not provide legal advice for any purpose, and neither creates nor constitutes evidence of an attorney-client relationship.