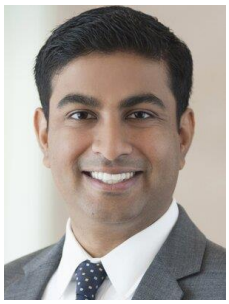
LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Rail Cos. Can Learn From Pipelines' TSA Cyber Compliance

By **Arjun Ramadevanahalli and Kirstin Gibbs** (November 7, 2022, 5:46 PM EST)



Arjun Ramadevanahalli

Kirstin Gibbs

Last month, the Transportation Security Administration issued its long-awaited cybersecurity rules for railroads under Security Directive 1580/82-2022-01.

The rail security directive applies to freight railroad carriers and other TSA-designated freight and passenger railroads, and reflects the TSA's continued expansion of its mandatory cybersecurity regulations across surface transportation modes.

The rail security directive is based on the same cybersecurity compliance framework that the TSA has deployed to the pipeline sector since July 2021. It also builds on the requirements issued to the rail industry last year concerning, among other things, cybersecurity incident response and reporting.

The rail security directive arrives amid a time of heightened vigilance against cyberattacks. In particular, malicious actors and nation-states are increasingly training their sights on domestic critical infrastructure.

In response, the federal government has stepped up efforts to meet the challenge. For example, the Biden administration has kicked off numerous 100-day sprints aimed at protecting the country's industry-based critical infrastructure sectors, such as the electric, water and chemical sectors.

But in a notable shift from previous practice, mandatory cybersecurity regulations — including the rail security directive — are also emerging as key components of the federal government's cybersecurity strategy.

Key Requirements

The rail security directive goes into effect immediately, and requires owners and operators to implement a suite of cybersecurity measures to protect their most operationally sensitive infrastructure. These measures include:

- Identification of key systems that, if compromised or exploited, could result in operational disruption;

- Development of network segmentation policies and controls to ensure that operational technology, or OT, systems can continue to safely operate in the event that an information technology, or IT, system has been compromised, and vice versa;

- Creation of access control measures to secure and prevent unauthorized access to key systems;

- Implementation of continuous monitoring and detection policies and procedures to detect cybersecurity threats; and

- The implementation of a risk-based security patch-management strategy.

Implementation

Many of the measures contained in the rail security directive are identical to those in Security Directive Pipeline-2021-02C, which applies to designated owners and operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.

The TSA issued the pipeline security directive on the heels of the 2021 ransomware attack on Colonial Pipeline Co., which led the pipeline to shut down operations and crippled fuel supplies on the Eastern Seaboard. The agency has revised the pipeline security directive several times, as it has refined its own compliance approach, and in response to significant industry pushback.

These changes are also apparent in the rail security directive. In particular, the rail security directive reflects the TSA's transition away from the prescriptive framework that beleaguered earlier iterations of the pipeline security directive, and toward a more flexible, performance-based approach that relies on the regulated entity presenting its compliance plan to the agency for approval.

Such compliance plans, known as cybersecurity implementation plans, are a core pillar of the rail security directive. They place the onus on carriers to explain to the TSA how they achieve — or will achieve in the future — the rail security directive's mandatory security outcomes.

Lessons From Pipeline Industry

The similarities between the TSA's pipeline security directive and rail security directive mean that railroad owners and operators can benefit from the pipeline industry's experience grappling with fundamental interpretation issues. Chief among these issues is determining the scope of the rail security directive.

Earlier iterations of the TSA's pipeline security directive staggered compliance deadlines differently for IT and OT systems. Mimicking the approach taken with the pipeline industry, the agency largely abandoned that approach for the rail security directive, and instead made its controls applicable to what the directive calls critical cyber systems — which include any IT or OT system that, if compromised or exploited, could create an operational disruption.

Owners and operators will need to carefully evaluate what constitutes an operational disruption, as defined in the rail security directive and in the context of their own operations, to establish a line of demarcation for the rollout of the rail security directive's mandatory controls.

Failure to do so can have significant cost impacts if the owner or operator needs to invest in additional

security tools or extend its implementation workplans. Additionally, owners and operators will need to consider critical data and business services supporting critical functions as they design their cybersecurity implementation plans.

The rail security directive also presents owners and operators with key decision points on the implementation of various security tools and strategies.

For example, the directive makes specific reference to the deployment of multifactor authentication. MFA is a security approach that requires users to authenticate themselves using two or more independent authentication factors — e.g., physical badge, pin and biometric scan.

The federal government has been a proponent of MFA — President Joe Biden even mandated MFA adoption for federal government systems in Executive Order No. 14028 — but some critical infrastructure owners have been wary of introducing added complexity to OT environments that have traditionally been secured through other means.

The rail security directive provides owner and operators with the flexibility to either deploy MFA to critical cyber systems, if not already in place, or to propose other controls commensurate to MFA. Thus, owners and operators who are not already compliant with the MFA requirement will need to balance the security benefits of adopting MFA against the costs and potential operational impacts of doing so in sensitive OT environments.

Owners and operators will need to carefully evaluate these decision points, and others like them, in preparing their cybersecurity implementation plans. And beyond implementation, owner and operators should also begin planning how they will keep compliance records.

Although the particulars around regulatory assessment and enforcement are unclear at this time, we expect that the TSA will eventually begin comprehensive auditing of owner and operator compliance with the rail security directive in the future. Keeping the audit trail in mind at an early stage can better prepare owners and operators to align their evidence with their cybersecurity implementation plans.

Next Steps

Rail owners and operators' cybersecurity implementation plans are due to the TSA by Feb. 21, 2023 — i.e., 120 days after the effective date of the rail security directive. Owners and operators that are unable to comply with all the directive's mandatory measures by then will have the opportunity to propose compliance timelines in their cybersecurity implementation plans.

When a carrier's cybersecurity implementation plan is approved by the TSA, the carrier will have 60 days to submit a plan to assess and audit its effectiveness in implementing the rail security directive's measures.

Separately, owners and operators should remain engaged with the TSA's administrative process as the agency continues to evolve its cybersecurity regulatory program. As was the case with the pipeline security directive, the TSA issued the rail security directive pursuant to its emergency authority that grants the agency's administrator the right to issue rules without providing notice or the opportunity for comment.

However, the TSA has indicated that it will also initiate a rulemaking to establish more formal

regulations that will allow owners and operators — and other interested parties — to weigh in on the agency's proposal during a public comment period.

Arjun Ramadevanahalli is an associate at Morgan Lewis & Bockius LLP.

Kirstin Gibbs is a partner, co-leader of the energy industry team, and leader of the climate change and sustainability working group at the firm.