BRACEWELL

INSIGHTS

TSA's New Cyber Directive for Freight & Passenger Railroad Carriers are the Agency's Latest Move to Keep the Nation on Track

October 31, 2022

By: ***Seth D. DuCharme***, ***Margaret B. Beasley*** *and* ***Anissa L. Adas***

In its continued efforts to enhance the cybersecurity of transportation and other critical infrastructure systems across the country, the Transportation Security Administration (TSA) issued on October 19, 2022 a new security ***directive*** for passenger and freight railroad carriers. The Enhancing Rail Cybersecurity – SD 1580/82-2022-01, which became effective October 24, will apply to approximately 80% of freight rail operators and 90% of passenger rail across the country. According to the TSA, the directive will implement requirements for passenger and freight railroad carriers that aim to "protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation's railroads."

TSA does not reinvent the wheel with this directive. Much like recent security ***directives*** aimed at critical pipeline operators, the new directive builds upon ***prior requirements*** for breach reporting and incident response plans and focuses on performance-based measures. The prior directive, issued in ***December 2021***, required relevant operators to (1) designate a cybersecurity coordinator; (2) report cybersecurity events to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours; (3) develop and implement a cybersecurity incident response plan; and (4) complete a cybersecurity vulnerability assessment.

In a ***press release***, TSA Administrator David Pekoske noted that the "nation's railroads have a long track record of forward-looking efforts to secure their network against cyber threats and have worked hard over the past year to build additional resilience, and this directive, which is focused on performance-based measures, will further these efforts to protect critical transportation infrastructure from attack."

The new TSA directive, developed in collaboration with CISA and the Federal Railroad Administration (FRA), seeks to achieve four security outcomes:

1. Establish network segmentation policies and controls to allow for the safe functioning of Operational Technology systems in the event of compromised networks.

2. Establish access control measures to prevent unauthorized access of Critical Cyber Systems.

3. Develop continuous monitoring and detection policies to identify threats and repair anomalies.

4. Mitigate risks of exploitation regarding unpatched systems by applying security patches, updates, and incorporating additional risk-based methodologies.

To reach these goals, the TSA directive imposes two primary requirements on passenger and freight rail operators, each of which will require numerous elements. First, these operators must, by February 21, 2023 (120 days after the effective date), develop a TSA-approved Cybersecurity Implementation Plan laying out specific measures the company is taking. Second, the operators must establish a Cybersecurity Assessment Program to include proactive testing and regular audits of cybersecurity upgrades and check for vulnerabilities. The TSA plans to initiate a rulemaking process and public comment period to create regulations in line with its security directives. Railroad carriers should remain aware of—and consider participating in the development of—this evolving guidance to ensure their cybersecurity response plans, and general cybersecurity practices, are compliant.

Though not as widely covered in the media as attacks on energy infrastructure like the Colonial Pipeline event, the rail industry has and will continue to face serious cybersecurity threats. For example, in April 2021, there was an attack on the Metropolitan Transportation Authority in New York by suspected state-linked hackers, and a ransomware attack against the Santa Clara Valley Transportation Authority.[1] Even aside from cyber threats, the rail industry—a crucial part of the nation's infrastructure—is under enormous pressure, as evidenced by the narrowly-avoided strike earlier this year that had the potential to completely disrupt the industry.[2] The Association of American Railroads welcomed the directive, stating: "Collaboration between railroads and government partners on these issues has a long, productive history that will continue to maintain and advance the smart, effective solutions to keep our network safe and freight moving. We appreciate the [TSA's] efforts on these important issues."[3]

More than a century and a half since the completion of the Transcontinental Railroad, railways continue to be a critical part of the country's infrastructure, and TSA's latest directive aims to ensure that they will remain so in the age of cyber threats.

[1] *See* **https://www.nytimes.com/2021/06/02/nyregion/mta-cyber-attack.html**; *see also* **https://www.ktvu.com/news/vtas-system-hacked-transit-officials-say-buses-light-rail-not-impacted**

[2] *See* **https://www.nytimes.com/2022/09/15/business/rail-strike.html**

[3] **https://www.aar.org/news/aar-statement-on-tsa-rail-cyber-directive/**