New Cyber Rules for Freight & Passenger Rail Announced

10.27.2022 | By Hon. Chris Carney

On October 18, 2022, the Transportation Security Administration (TSA) issued Security Directive 1580-21-01A, intended to make the nation's rail system more cyber secure by promoting lines of communication and improving response. In the face of on-going cybersecurity threats to computer systems that control surface transportation modes, including rail, TSA – in conjunction with the Cybersecurity and Infrastructure Security Agency (CISA) – is circulating this new security directive for all freight railroad carriers described in 49 CFR 1580.101, as well as all other TSA-designated rail systems to include:

- intercity, commuter and short-haul passenger train service providers;
- rail transit systems; and
- rail operations at certain fixed-site facilities that ship or receive specified hazardous materials by rail.

Security Directive Took Effect October 24, 2022

The Directive requires owner/operators of the rail systems to:

- Designate a cybersecurity coordinator who is available to be contacted by TSA and CISA 24-hours a day, seven days a week to serve as a single point of contact to these agencies on all cyber issues;
- Report any cybersecurity incidents to CISA;
- Develop a cybersecurity incident response plan to help rapid recovery from cyberattacks; and
- Conduct cybersecurity vulnerability assessments as specified by TSA to evaluate current security practices and to identify gaps in security and recovery/mitigation actions.

Owner/operators will be required to report all cybersecurity incidents no later than 24-hours after the event, but ideally as soon as is possible. Incidents include unauthorized access to critical information and/or operating systems, discovery of malicious software, any denial of service attack and any other cyber event that results in operational disruption to freight and passenger rail systems to CISA.

In addition, owner/operators are required to conduct exercises at least annually that test the effectiveness of cyber response procedures, plans and personnel. Owner/operators not previously required by TSA to develop and submit a Cybersecurity Incident Response Plan have 180 days (beginning on October 24th) to do so.

This security directive is quite specific as to the responsibilities of the rail systems, and clearly identifies what rail systems must do. While this could be taken to suggest rail owner/operators will face increased litigation risk if they are found to be non-compliant when an incident occurs, the directive does not identify any penalties for non-compliance.