Contact Public Affairs

TSAmedia@tsa.dhs.gov

PRESS RELEASE

FOR IMMEDIATE RELEASE **Oct. 23, 2023**

TSA renews cybersecurity requirements for passenger and freight railroad carriers

Requirements seek to reduce the risk cybersecurity threats pose to critical railroad operations and facilities

WASHINGTON — The Transportation Security Administration (TSA) announced updates to three security directives (SD) regulating passenger and freight railroad carriers in the continued effort to enhance the cybersecurity of surface transportation systems and associated infrastructure. These revised directives, which were set to expire on Oct. 24, have been renewed for one year, and include updates that seek to strengthen the industry's defenses against cyberattacks.

Developed with comprehensive input from industry stakeholders and federal partners, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the Department of Transportation's Federal Railroad Administration (FRA), the three security directives further enhance cybersecurity preparedness and resilience for the nation's critical railroad operations. It requires TSA-specified passenger and freight railroad carriers to take action to prevent disruption and degradation to their infrastructure with a flexible, performance-based approach, consistent with TSA's requirements for pipeline operators.

"The renewal is the right thing to do to keep the nation's railroad systems secure against cyber threats, and these updates sustain the strong cybersecurity measures already in place for the railroad industry," said TSA Administrator David Pekoske. "TSA's partnerships with CISA, FRA and the railroad industry have been, and will continue to be, instrumental in our work towards strengthening resilience and preventing harm."

The revised security directives, *Enhancing Rail Cybersecurity,* and the revised SD series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, include a requirement for covered owners and operators to test a minimum of two objectives in their Cybersecurity Incident Response Plan every year. They also require including employees who have been identified by their positions as active participants in these exercises.

The revised security directive series, *Rail Cybersecurity Mitigation Actions and Testing*, also requires railroad owners and operators to annually submit an updated Cybersecurity Assessment Plan to TSA for review and approval and report the results from the previous year using a

schedule for assessing and auditing specific cybersecurity measures for effectiveness such that all cybersecurity measures are assessed within a three-year period.

To view TSA's security directives and guidance documents, please visit: TSA Cybersecurity Toolkit or https://www.tsa.gov/sd-and-ea.

###