Updates
February 10, 2023

New TSA Rail Cybersecurity Rule Shows Trend Toward Prescriptive Mandates

Background

Critical infrastructure providers confront unique cyber threats. The use of operational technology (OT) introduces risks that arise from, for example, legacy equipment that cannot readily be patched, updated, or replaced. Because OT controls physical machines, exploitation of vulnerabilities can cause cascading and potentially catastrophic effects. In response to escalating risk in this area, the U.S. government has increased its efforts to enhance critical infrastructure cybersecurity.

As part of that effort, the Transportation Security Administration (TSA) issued a new security directive (SD) on October 18, 2022, to enhance cybersecurity preparedness and resilience for designated passenger and freight railroads. The SD was developed with extensive input from industry stakeholders and federal agencies including the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Railroad Administration (FRA). It adopts a layered, defense-in-depth approach.

The SD supports the Biden administration's efforts to shore up essential infrastructure against cyber attacks and updates prior requirements. In December 2021, the TSA issued two SDs that required specified surface transportation entities to implement urgently needed measures to immediately enhance the cybersecurity of the surface transportation sector. In July 2022, after the 2021 Colonial Pipeline ransomware attack, the TSA issued revised cybersecurity requirements for U.S. pipeline operators with a focus on performance-based measures to achieve critical cybersecurity outcomes. More recently, on October 12, 2022, the TSA announced plans to issue new cybersecurity requirements for critical aviation systems after several U.S. airport websites were hit with apparently coordinated denial-of-service attacks. These directives demonstrate the Biden administration's continued effort to further cybersecurity resiliency for the nation's infrastructure, which we expect to accelerate.

To Whom Does the Directive Apply?

The SD applies to all freight railroad carriers (Owner/Operators) subject to the previous Security Directive 1580-21-01, as well as other TSA-designated freight and passenger railroads based on a risk determination. The TSA will notify such Owner/Operators and provide specific compliance deadlines for the requirements in the directive.

Security Directive 1580/82-2022-01: Rail Cybersecurity Mitigation Actions and Testing

The SD requires TSA-specified passenger and freight railroad carriers to take action to prevent disruption and degradation to the rail infrastructure. The SD mandates that these Owner/Operators implement two overarching cybersecurity measures meant to prevent disruptions to their infrastructure and operations.

First, the SD requires covered Owner/Operators to establish and execute a TSA-approved Cybersecurity Implementation Plan (CIP) that describes the specific cybersecurity measures the passenger and freight rail carriers are using and also sets forth certain standards these carriers must include in the CIP to do the following:

- Identify "Critical Cyber Systems," as defined in the SD.
- Implement network segmentation policies and controls to prevent OT disruption caused by information technology (IT) compromise, and vice versa.
- Create and implement access controls to prevent unauthorized access to critical cyber systems.
- Ensure that these critical systems are covered by continuous monitoring and detection policies and procedures to detect threats.
- Apply security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology.

The CIP, which sets the standards that covered entities must satisfy, requires TSA approval. The TSA has the authority to inspect covered entities for compliance with their approved CIPs. The CIP requirements are extensive and detailed and are more prescriptive than most current federal cybersecurity rules.

Second, covered Owner/Operators must establish a Cybersecurity Assessment Program (CAP) and submit an annual plan for the CAP. The CAP must proactively assess and audit cybersecurity measures and will track an Owner/Operator's CIP. The CAP will also entail an initial architectural design review as prescribed by the TSA and include penetration testing and other assessment tools.

Changes From the Last Directive

The new SD builds upon the TSA's performance-based security initiative. Security Directive 1580-2021-01, issued last December, detailed four requirements for Owner/Operators to implement: (1) designate a cybersecurity coordinator; (2) report cybersecurity incidents to CISA; (3) implement an incident response plan; and (4) complete a cybersecurity vulnerability assessment. It was meant to take a more flexible approach to the two earlier directives of 2021 and to account for the IT structure specific to industrial control systems, including operational technology and IT. Tom VanNorman, a senior vice president at GRIMM Cyber who specializes in Industrial Control Systems (ICS) and OT in critical infrastructure, notes that the new SD sets out more specific requirements relating to network inventory, asset visibility and monitoring, and patching. Whereas prior SDs contained generalized recommendations for good cybersecurity practices and were sometimes criticized for failing to account for OT-specific considerations, the TSA's new approach is more targeted, prescriptive, and specific to the problem set, while still leaving room for Owner/Operators to develop cybersecurity programs that are appropriate to their systems and risk profiles. The new SD also signals an increased focus on compliance than previous iterations.

Implementation

Under the SD, the TSA has notified or will notify covered Owner/Operators that they are subject to the new rules. Such Owner/Operators must immediately acknowledge receipt via email as outlined in the notification. Owner/Operators must then submit a CIP for TSA approval no later than February 21, 2023, which is 120 days after the effective date of the SD. This aggressive timeline may be challenging for Owner/Operators who do not already have a plan in place, particularly smaller operators with limited resources. VanNorman suggests to meet the implementation timelines, Owner/Operators should focus on their organization's highest-value assets, prioritize protection measures such as monitoring and patching to match, and design appropriate policies and

control measures to mitigate cybersecurity-related risks.

No later than 60 days after the TSA's approval of an Owner/Operator's CIP, the Owner/Operator must submit an annual plan describing how they will carry out their CAP, which measures the effectiveness of the CIP. This annual plan must include the schedule for specific actions and must be updated on an annual basis.

Takeaway

Critical infrastructure cybersecurity has gained prominence in the news and among policymakers in recent years. It will remain a principal focus in the security community and among regulators. Businesses in critical infrastructure will need to keep up with the different requirements and the timelines associated with these implementation plans. The TSA also intends to begin a rulemaking process, which would establish regulatory requirements for the rail sector following a public comment period.

Recent media reports indicate that the federal government will continue to roll out prescriptive, mandatory security rules rather than relying on reporting requirements and voluntary adoption of security measures. This effort will initially leverage individual agencies' existing regulatory authority. Industry should expect those agencies to become increasingly active in promulgating rules and potentially using enforcement authorities to promote compliance.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Oviett Worthington Wargula

Associate
OWorthingtonWargula@perkinscoie.com 206.359.3130

Explore more in

Infrastructure Development Privacy & Security Technology Transactions & Privacy Law Communications

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights