wiley

NEWSLETTER

TSA Rail Cybersecurity Directives Show Increasing Government Regulation of Critical Infrastructure and the Private Sector

December 2021

Privacy In Focus®

What: The Transportation Security Administration (TSA) has issued two Security Directives aimed at passenger and freight railroad cybersecurity, continuing the government's move to an increasingly regulatory approach to private sector cybersecurity. Security Directive 1582-21-01, "Enhancing Public Transportation and Passenger Railroad Cybersecurity"[1] applies to each owner/operator of a passenger railroad carrier or rail transit system[2] while Security Directive 1580-21-01, "Enhancing Rail Cybersecurity"[3] applies to freight railroad carriers.[4] Both directives require reporting the same information to the government to prevent the significant harm that could come from the degradation, destruction, or malfunction of the systems that control rail transit.

What does it mean for industry: The Security Directives build upon pipeline security directives issued after the Colonial Pipeline ransomware attack in May 2021.[5] The rail Security Directives are effective on December 31, 2021 and require that railroad owner/operators perform four critical actions: (1) designate a Cybersecurity Coordinator; (2) report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA); (3) develop a Cybersecurity Incident Response Plan; and, (4) conduct a cybersecurity vulnerability assessment using a form provided by TSA.[6] The Security Directives require rail owner/operators to report cybersecurity incidents to CISA, which will share reported information with TSA. TSA and CISA will use the information for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other actions that

Authors

Jacqueline F. "Lyn" Brown
Special Counsel
202.719.4114
jfbrown@wiley.law

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Cybersecurity
Privacy, Cyber & Data Governance

they believe may help prevent cybersecurity incidents.

What do the TSA Rail Security Directives do?

TSA has found that cybersecurity incidents affecting surface transportation are a growing and evolving threat.[7] TSA believes that malicious cyber actors continue to target U.S. critical infrastructure, including freight railroads, passenger railroads, and rail transit systems, with cyberattack and cyber espionage campaigns to seek political, economic, and military advantage over the United States and its allies. [8] As a result, the two (2) Security Directives mandate that owners/operators of "higher risk" railroads and transit implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.

Critical Action Rail Owners/Operators are Required to Perform

Both the rail passenger and rail freight Security Directives are effective on December 31, 2021 and contain identical requirements. Under the Security Directives railroad owner/operators must perform four critical actions:

- Designate a Cybersecurity Coordinator;
- Report cybersecurity incidents to the CISA;
- Develop a Cybersecurity Incident Response Plan; and,
- Conduct a cybersecurity vulnerability assessment using the form provided by TSA.[9]

These requirements necessitate immediate action by entities that are directly covered by the Security Directives, and are instructive for other private sector organizations that are looking ahead to manage regulatory risk related to cybersecurity.

Reportable Cybersecurity Incidents:

Organizations often grapple with what makes an incident reportable, and this challenging question is presently being debated in Congress as incident reporting mandates are included in pending legislation.

Both Security Directives mandate reporting to CISA[10] certain cybersecurity incidents, which are loosely defined to include the following:

- Unauthorized access of an Information or Operational Technology system;
- Discovery of malicious software on an Information or Operational Technology system;
- Activity resulting in a denial of service to any Information or Operational Technology system;
- Any other cybersecurity incident that results in operational disruption to the Owner/Operator's rail systems or facilities;
- An incident that has the potential to cause impact to a large number of passengers, critical infrastructure;

- An incident that impacts national security, economic security, or public health and safety.

Cybersecurity incidents report must be reported as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.[11] Reports must be made to CISA using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870.

Directives are part of the government's increasingly aggressive efforts to address cybersecurity threats to critical infrastructure and the private sector

The Security Directives are part of an ongoing effort by the government to increase the cybersecurity readiness of critical infrastructure and the private sector to protect the economy and national security. In November 2021, CISA released the Federal Government Cybersecurity Incident and Vulnerability Playbooks as part of the Biden Administration's efforts to improve the nation's cybersecurity in accordance with Executive Order 14028. When they were published, CISA encouraged all public and private sector partners to review the Playbooks to check their own vulnerability and incident response practices. The Playbooks then, are required for federal civilian executive branch agencies but recommended for private industry as best practices.

On July 28, 2021, the President issued a National Security Memorandum (NSM), entitled "Improving Cybersecurity for Critical Infrastructure Control Systems" stating:

The cybersecurity threats posed to the systems that control and operate the critical infrastructure on which we all depend are among the most significant and growing issued confronting our Nation. The degradation, destruction, or malfunction of systems that control this infrastructure could cause significant harm to the national and economic security of the United States. [12]

The Administration is, therefore, attempting to safeguard the critical infrastructure of the Nation, with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions defined as those functions so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, and/or public health or safety. [13]

For critical infrastructure, however, the government is using its authorities to mandate cybersecurity preparedness and readiness. After Colonial Pipeline became the victim of a highly publicized ransomware attack that shut down the major gasoline and fuel pipeline along the Atlantic coast,[14] TSA issued a Security Directive to owners and operators of hazardous liquid and natural gas pipelines and facilities mandating that they take certain preventative actions. TSA is now exercising its authorities to assess threats to transportation and enforce security-related regulations and requirements to issue these security directives to rail transit owners/operators to immediately protect transportation security.[15] TSA has similar national emergency powers with respect to maritime transportation, including port security, and may soon seek to issue additional Security Directives to enhance cybersecurity efforts in maritime cargo shipping, navigation or communication, commercial fishing, or cruise lines.

Key Takeaways

Wiley continues to advise companies across the economy to take a risk-management approach to maintaining reasonable cybersecurity programs. In the absence of comprehensive federal law or applicable sector-specific requirements, companies can look to federal contracting requirements, NIST publications, and governmental regulatory action, such as Security Directives issued to the transportation sector, for guidance to build effective and defensible programs. Such programs need to adapt to new threats and to new indications from federal and state governments of regulatory risk.

We see a substantial growth in governmental regulatory and oversight in cybersecurity given concerns about critical infrastructure, worries about software security, the growth in ransomware attacks, and the government's increasing aggressive approach. Federal regulators are increasingly using varied authorities to demand that companies address the threats posed by outdated industrial and operational controls, software vulnerabilities, and ransomware attacks.

The private sector can help protect against regulatory scrutiny, civil enforcement actions, and litigation by reviewing their current cybersecurity requirements, utilizing the CISA Playbooks, and looking to governmental cues like the newly issued Security Directives. Wiley encourages all organizations to consider how their security programs, incident response plans, and relationships with government (both regulators and law enforcement) compare to the ever-evolving government expectations as federal departments and agencies look to establish and shape standards of care for risk management and cyber incident reporting and response.

---

[1] https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf

[2] 49 CFR 1582.101.

[3] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf

[4] 49 CFR 1580.101.

[5] https://www.govinfo.gov/content/pkg/FR-2021-09-24/pdf/2021-20738.pdf

[6] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf (*see* p.1-3).

[7] https://omb.report/icr/202111-1652-003/doc/116791301, p.2.

[8] https://omb.report/icr/202111-1652-003/doc/116791301, p.2.

[9] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf (*see* p.1-3).

[10] The information reported to CISA pursuant to the SD is shared with TSA and may also be shared with the National Response Center (NRC). *See* OMB control number 1670-0037.

[11] *See* SD 1580-21-01, Actions Required (B)(2).

[12] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[13] https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/. The NSM also announced an Industrial Control Systems Cybersecurity Initiative to defend the U.S.' critical infrastructure by encouraging and facilitating deployment of technologies and systems that provide threat visibility, indications, detection, and warnings, and that facilitate response capabilities for cybersecurity in essential control systems and operational technology networks. The Initiative, however, is a voluntary, collaborate effort between the Federal Government and the critical infrastructure community to significantly improve the cybersecurity of these critical systems. *See* NSM, Section 2. https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/fact-sheet-biden-administration-announces-further-actions-to-protect-u-s-critical-infrastructure/

[14] https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack

[15] 49 USC 114(d) (f) (l).