Cybersecurity, Privacy &
Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

TSA Mandates Immediate Cyber Preparations for Rail Owners and Operators following its Imposition of Similar Requirements on Airports and Airlines

January 6, 2022

Key Points

- This December, the Transportation Security Administration (TSA) issued a pair of Directives establishing cybersecurity measures for high-risk freight rail, passenger rail, and rail transit owners and operators. These directives went into effect December 31, 2021. Specifically, owners and operators must: (1) name a cybersecurity coordinator; (2) report any cyber incidents within 24 hours to the Cybersecurity and Infrastructure Security Agency (CISA); (3) develop an incident response plan; and (4) complete a cybersecurity vulnerability assessment.
- At the same time, TSA issued an Information Circular recommending that lower-risk rail owners and operators and over-the-road bus owners and operators implement the above requirements voluntarily.
- TSA had previously directed airports and airline operators to (1) name a cybersecurity coordinator; and (2) report cyber incidents within 24 hours to CISA.
- The resulting deadlines for applicable rail owners and operators are the following:
  - January 7, 2022 – Designate a cybersecurity coordinator
  - March 31, 2022 – Conduct cybersecurity vulnerability assessment
  - June 29, 2022 – Implement a cyber incident response plan

Background

On December 2, 2021, the Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), announced two new Directives (the Directives) mandating cybersecurity measures for critical surface transportation systems. The Directives' requirements cover owners and operators of high-risk freight railroads, passenger rail and transit. TSA also issued an information circular calling for low risk rail owners and operators and over the road bus owners and operators (those not covered by the first two Directives) to voluntarily adopt the same cybersecurity measures.

Contact Information

If you have any questions concerning this alert, please contact:

Natasha G. Kohne
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
mreed@akingump.com
Dallas
+1 214.969.2713

Susan H. Lent
slent@akingump.com
Washington, D.C.
+1 202.887.4558

Lauren E. York
lyork@akingump.com
Dallas
+1 214.969.4395

These Directives follow the TSA's recent updates to its aviation security programs to require that airport and airline operators implement the first two provisions above. They also represent the TSA's second round of cybersecurity directives in 2021, arriving after the two pipeline requirement announcements in May and July.

The TSA immediately implemented these new requirements, which took effect on December 31.

Scope and Requirements

High-Risk Freight Rail, Passenger Rail, and Rail Transit Operators Requirements

The first Directive, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, covers owners and operators of passenger railroad or rail-transit systems identified in 49 C.F.R. § 1582.101, while the second Directive, *Enhancing Rail Cybersecurity*, applies to freight railroads identified in 49 C.F.R. § 1580.101. According to the press release, these represent "higher-risk" freight railroads, passenger rail and rail transit.[1]

The Information Circular, *Enhancing Surface Transportation Cybersecurity* (the voluntary Directive) recommends but does not require that those owners and operators not covered by the first two Directives implement the same cybersecurity measures. These "lower-risk" transport systems include railroad owners and operators identified in 49 C.F.R. § 1580.1(a), passenger railroads, public transport agencies or rail transit system owners and operators identified in 49 C.F.R. § 1582.1, and over-the-road-bus owners and operators identified in 49 C.F.R. § 1584.1.

A "cybersecurity incident" under the Directives includes any event that "jeopardizes, disrupts or otherwise impacts the integrity, confidentiality, or availability of computers, information or communications systems or networks" including any physical and virtual infrastructure those systems control or information resident on the system, or events under investigation as incidents.[2] The Directives require owners and operators to adopt the following measures:

1. **Designate a Cybersecurity Coordinator**– by January 7, 2022 (seven days after the December 31 effective date) owners and operators must designate a Cybersecurity Coordinator available "at all times" to serve as the principal point of contact with the TSA and CISA while coordinating cybersecurity practice and managing cybersecurity incidents. The name, title, phone number and email address of both the coordinator and at least one alternate must be emailed to the TSA.[3]
2. **Report Cybersecurity Incidents to CISA within 24 hours**– the Directives define cybersecurity incidents very broadly, even covering events that are being investigated as "a possible cybersecurity incident." Incidents must be reported to CISA "as soon as practicable but no later than 24 hours" after they are identified.[4]
3. **Develop and Implement a Cybersecurity Risk Response Plan**– by June 29, 2022 (180 days from the effective date), owners and operators must have a plan to reduce the risk of operational disruption in the event of a cybersecurity incident affecting their systems. Once the plan is in place, owners and operators will have 7 days to certify it with the TSA.[5]

4. **Complete a Cybersecurity Vulnerability Assessment**– by March 31, 2022 (90 days from the effective date), owners and operators must conduct and submit a cybersecurity vulnerability assessment which will include: an evaluation of current practices and activities to address cyber risks, identification of gaps in current cybersecurity measures, identification of remediation measures to address gaps and a plan to implement these measures.[6]

The Directives contain a host of other requirements, such as:

- immediately sending confirmation of receipt of these Directives to the TSA via email
- immediately passing on the Directives' measures to senior management and any personnel responsible for implementing them, and
- immediately sending emailing notification to TSA if unable to perform any of the requirements.[7]

CISA and the TSA will share information furnished under these requirements with each other, and may share with the National Response Center and "other agencies as appropriate."[8]

Requirements for Airports and Airlines

TSA previously imposed requirements on airport and airline operators to (1) designate a cybersecurity coordinator and (2) report cybersecurity incidents to CISA within 24 hours of identifying them.[9] The TSA also noted that it plans to expand these aviation requirements at a later date, along with issuing guidance to smaller operators.

Takeaway

This announcement reflects a continuation of the TSA's effort to bring stronger cybersecurity measures to critical infrastructure. Since the May and July cybersecurity directives following the Colonial Pipeline ransomware incident, DHS has been vocal about the need to mitigate the cyber threats to infrastructure and transportation and companies have been required to invest millions of dollars in enhanced cybersecurity protections. The federal government as a whole has likewise taken up this cause, with such actions as the White House Executive Order on cybersecurity threat response, as well as cyber protections in the recently passed Infrastructure Investment and Jobs Act.

Companies at every level of the infrastructure and transportation sector, as well as other sectors, should review their cybersecurity practices to ensure compliance with existing mandates and expect further mandates in the near future. The requirements will most likely be iterative and will require close coordination with advisors to ensure proper procedures and protocols are set up to comply.

Please contact a member of Akin Gump's cybersecurity, privacy and data protection team if you have any questions about this alert or how these new requirements will affect your company.

[1] Press Release, U.S. Dept. of Homeland Security, *DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators* (December 2, 2021) hereinafter "press release." available at https://www.dhs.gov/news/2021/12/02/dhs-announces-new-cybersecurity-requirements-surface-transportation-owners-and.

[2] Transportation Security Administration, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, Security Directive 1582-21-01 (December 2, 2021) available at https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

[3] *Id*. at 2.

[4] *Id*. at 3.

[5] *Id*. at 5.

[6] *Id*. at 6.

[7] *Id*.

[8] *Id*. at 2.

[9] Press Release at 1. For more information on security requirements for airport and airline operators, please review the TSA Aviation Program page available at https://www.tsa.gov/for-industry/aviation-programs.

akingump.com