AMERICAN PUBLIC TRANSPORTATION ASSOCIATION
FACT SHEET
U.S. DEPARTMENT OF HOMELAND SECURITY
TRANSPORTATION SECURITY ADMINISTRATION SECURITY DIRECTIVE
ENHANCING PUBLIC TRANSPORTATION AND PASSENGER RAILROAD CYBERSECURITY
December 3, 2021

On December 2, 2021, the Transportation Security Administration (TSA) issued Security Directive 1582-21-01: Enhancing Public Transportation and Passenger Railroad Cybersecurity for each owner/operator of a passenger railroad carrier or rail transit system identified in 49 CFR 1582.101. The Security Directive is being issued under the authority of 49 U.S.C. § 114(l)(2)(A) and goes into effect on December 31, 2021.

The Security Directive requires the owner/operator of an applicable passenger railroad carrier or rail transit system, to:

- Designate a Cybersecurity Coordinator;
- Report cybersecurity incidents[1] to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) no later than 24 hours after a cybersecurity incident is identified;
- Develop and adopt a Cybersecurity Incident Response Plan; and
- Conduct a Cybersecurity vulnerability assessment using a form provided by TSA.

All information reported to TSA or CISA is subject to Protections of Sensitive Security Information.[2]

Required Actions

- **Cybersecurity Coordinator**. An owner/operator must designate both a primary and at least one alternate Cybersecurity Coordinator at the corporate level to serve as the primary contact(s). Coordinators must be accessible 24 hours a day, seven days a week to TSA and CISA and to coordinate cyber and related emergency response practices and procedures and work with appropriate law enforcement and emergency response agencies. The Cybersecurity Coordinators must be U.S. citizens, eligible for a security clearance, and identified to TSA within **seven days** of the effective date of the Security Directive.[3]

---

[1] A cybersecurity incident means an event that, without lawful authority, jeopardizes, disrupts, or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the owner/operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).
[2] 49 CFR 1520, Protection of Sensitive Security Information. This part governs the maintenance, safeguarding, and disclosure of records and information that TSA has determined to be Sensitive Security Information (SSI).
[3] Owner/operators must submit the Cybersecurity Coordinator's information via email to TSA-Surface-cyber@tsa.dhs.gov.

- **Reporting.** An owner/operator must report to CISA **no later than 24 hours** after a cybersecurity incident is identified involving:[4]

    - Unauthorized access of an Information Technology (IT) or Operational Technology (OT) systems;
    - Discovery of malicious software on an IT or OT system;
    - Activity resulting in denial of service to any IT or OT systems; and
    - Any other cybersecurity incident that results in operation disruption to IT or OT systems, rail systems or facilities, or an incident that has the potential to cause impact to a large number of passengers, critical infrastructure or core government functions, or impacts national security, economic security, or public health and safety.

- **Cybersecurity Incident Response Plan**. An owner/operator must develop and adopt **within 180 days** of the effective date of the Security Directive a Cybersecurity Incident Response Plan that includes measures to reduce the risk of operational disruption, or other significant business or functional degradation to necessary capacity, should the rail system or facility experience a cybersecurity incident. In addition, an owner/operator must conduct situational exercises to test the effectiveness of procedures, and personnel responsible for implementing the measures in the plan, no less than annually. Within **seven days** of completing the requirements of this section, an owner/operator must submit a statement to TSA certifying that it has met the requirements.[5]

- **Cybersecurity Vulnerability Assessment**. An owner/operator must submit a cybersecurity vulnerability assessment and identify gaps using the form[6] provided by TSA **within 90 days** of the effective date of the Security Directive.[7] The form utilizes the functions and categories found in the National Institute of Standards and Technology (NIST) Cybersecurity Guidance Framework.

Alternative Measures

An owner/operator must immediately notify TSA via email if it is unable to implement any of the measures in the Security Directive and may provide a proposed alternative measure for TSA approval.[8]

[4] Reports must be made to CISA Central using CISA's Incident Reporting form to: https://us-cert.cisa.gov/forms/report or calling (888) 282-0870.
[5] Owner/operators must submit statements certifying that they have met the requirements of the Cybersecurity Incident Response Plan via email to SurfOpsRail-SD@tsa.dhs.gov
[6] TSA cybersecurity vulnerability assessment and supporting materials: Cybersecurity Measures for Surface Modes - OMB 1652-0074.
[7] Owner/operators must submit the TSA cybersecurity vulnerability assessment via email to SurfOpsRail-SD@tsa.dhs.gov.
[8] Immediate notification and approval of alternative measures submitted via email to TSA-Surface-Cyber@tsa.dhs.gov.