U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

SECURITY DIRECTIVE

NUMBER	Security Directive 1582-21-01
SUBJECT	Enhancing Public Transportation and Passenger Railroad Cybersecurity
EFFECTIVE DATE	December 31, 2021
EXPIRATION DATE	December 31, 2022
CANCELS AND SUPERSEDES	Not Applicable
APPLICABILITY	Each owner/operator identified in 49 CFR 1582.101 that is a passenger railroad carrier or rail transit system
AUTHORITY	49 U.S.C. 114(d), (f), (*l*) and (m)
LOCATION	All locations within the United States

PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this security directive due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to prevent against the significant harm to the national and economic security of the United States that could result from the "degradation, destruction, or malfunction of systems that control this infrastructure." *See National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021). This Security Directive is being issued under the authority of 49 U.S.C. 114(*l*)(2)(A).[1]

This Security Directive, which applies to all Public Transportation/Passenger Rail (PTPR) owner/operators identified in 49 CFR 1582.101 that own or operate a passenger railroad or a rail transit system [2] requires four critical actions:

---

[1] This provision from section 101 of the Aviation and Transportation Security Act, Pub. L. 107-71 (115 Stat. 597; Nov. 19, 2001), states: "Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary."

[2] The applicability does not include bus-only operations. In addition, section 114(d) provides the Administrator of TSA the authority for security of all modes of transportation; section 114(f) provides specific additional duties and powers to the Administrator; 114(m) provides authority for the Administrator to take actions that support other agencies.

1. Designate a Cybersecurity Coordinator who is required to be available to TSA and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) at all times (all hours/all days) to coordinate implementation of cybersecurity practices, and manage of security incidents, and serve as a principal point of contact with TSA and CISA for cybersecurity-related matters;

2. Report cybersecurity incidents to CISA;

3. Develop a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should their Information and/or Operational Technology systems be affected by a cybersecurity incident; and

4. Conduct a cybersecurity vulnerability assessment using the form provided by TSA and submit the form to TSA. The vulnerability assessment will include an assessment of current practices and activities to address cyber risks to Information and Operational Technology systems, identify gaps in current cybersecurity measures, and identify remediation measures and a plan for the Owner/Operator to implement the remediation measures to address any identified vulnerabilities and gaps.[3]

To avoid duplicate reporting, information provided to CISA pursuant to this Security Directive will be shared by CISA with TSA and may also be shared with the National Response Center and other agencies as appropriate. Similarly, information provided to TSA pursuant to this Security Directive will be shared with CISA and may also be shared with the National Response Center and other agencies as appropriate.[4] All information that must be reported to TSA or CISA pursuant to this Security Directive is sensitive security information subject to the protections of 49 CFR part 1520.

TSA and CISA will use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.

ACTIONS REQUIRED

A. Cybersecurity Coordinator

1. Owner/Operators must designate and use a primary and at least one alternate Cybersecurity Coordinator at the corporate level.

2. Owner/Operators must provide in writing to TSA, at TSA-Surface-Cyber@tsa.dhs.gov, the names, titles, phone number(s), and email address(es) of the Cybersecurity Coordinator and alternate Cybersecurity Coordinator(s) required by paragraph A.1. within seven days of the effective date of this Security Directive, commencement of new

[3] This form has received emergency approval from the Office of Information and Regulatory Affairs. See OMB Control No. 1652-0074, expiration date May 31, 2022.
[4] Presidential Policy Directive (PPD)-41 calls for federal cyber incident response agencies to share incident information with each other to achieve unity of governmental effort. *See* PPD-41 at section III.D.

operations, or change in any of the information required by this section.

3. The Cybersecurity Coordinator and alternate must—

   a. Be a U.S. citizen who is eligible for a security clearance;

   b. Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and CISA;

   c. Be accessible to TSA and CISA 24 hours a day, seven days a week;

   d. Coordinate cyber and related security practices and procedures internally; and

   e. Work with appropriate law enforcement and emergency response agencies.

B. Reporting Cybersecurity Incidents

1. Owner/Operators must report cybersecurity incidents to CISA involving systems that the Owner/Operator has responsibility to operate and/or maintain including:

   a. Unauthorized access of an Information or Operational Technology system;

   b. Discovery of malicious software on an Information or Operational Technology system;

   c. Activity resulting in a denial of service to any Information or Operational Technology system; and/or

   d. Any other cybersecurity incident that results in operational disruption to the Owner/Operator's Information or Operational Technology systems or other aspects of the Owner/Operator's 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.

2. Owner/Operators must report the incidents required by this section as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.

3. Reports required by this section must be made to CISA Central using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870.[5] All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

4. The report to CISA must include the following information, as available to the reporting

[5] CISA's Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of the security incidents Railroads and Rail Transit Agencies must report pursuant to this Security Directive as well as the ability to conduct improved analysis.

Owner/Operator at the time of the report:

a. The name of the reporting individual and contact information, including a telephone number and email address. The report must also explicitly specify that the information is being reported in order to satisfy the reporting requirements in this Security Directive.

b. The affected rail system(s) or facilities, including identifying information and location.

c. Description of the threat, incident, or activity, to include:

i. Earliest known date of compromise;

ii. Date of Detection;

iii. Information about who has been notified and what action has been taken;

iv. Any relevant information observed or collected by the Owner/Operators, such as malicious IP addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts; and

v. Any known threat information, to include information about the source of the threat or attack, if available.

d. A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual or imminent adverse impacts to service operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident.

5. A description of all responses that are planned or under consideration, to include, for example, a reversion to manual operations of train movement and control, if applicable.

6. Any additional relevant information. If all the required information is not available at the time of reporting, Owner/Operators must submit an initial report within the specified timeframe and supplement as additional information becomes available.

7. TSA will accept a report to CISA by an Owner/Operator of a cybersecurity incident under this section as satisfying the reporting requirement to TSA under 49 CFR 1570.203, for the same incident, if the report to CISA explicitly specifies that the information is being reported in order to satisfy the reporting requirements in this Security Directive.

C. Implementing a Cybersecurity Incident Response Plan

1. Within 180 days from the effective date of this Security Directive, unless otherwise directed, Owner/Operators must develop and adopt 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 their rail system or facility experience a cybersecurity incident. The Cybersecurity Incident Response Plan must provide specific measures sufficient to ensure the following objectives, as technically applicable and feasible:

    a. Prompt identification, isolation and segregation of the infected systems from uninfected systems, networks, and devices to prioritize:

        i. Limiting the spread of autonomous malware,

        ii. Denying continued attacker access to systems,

        iii. Determining extent of compromise, and

        iv. Preservation of evidence or partially encrypted data system storage.

    b. Security and integrity of backed-up data, including measures to secure and safely maintain backups offline, and implement procedures requiring scanning of stored backup data with host security software to check that it is free of malicious artifacts when the backup is made and when tested for restoration.

    c. Established capability and governance for isolating the Information Technology and Operational Technology systems in the event of a cybersecurity incident that arises to the level of potential operational disruption while maintaining operational standards and limits.

2. The Cybersecurity Incident Response Plan must, at a minimum, identify who (by position) is responsible for implementing the specific measures and any necessary resources needed to implement these measures.

3. The Owner/Operator must conduct situational exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in the Cybersecurity Incident Response Plan, no less than annually.

4. Within 7 days of completing the requirements in this section (section C.), Owner/Operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA at SurfOpsRail-SD@tsa.dhs.gov certifying the Rail Owner/Operator has met the requirements. Documentation of compliance must be provided to TSA upon request and without a subpoena.

D. Cybersecurity Vulnerability Assessment

1. Owner/Operators must complete a cybersecurity vulnerability assessment and identify cybersecurity gaps using a form provided by TSA. The form utilizes the functions and

categories found in the National Institute of Standards and Technology (NIST) Cybersecurity Guidance Framework.

2. Owner/Operators must identify remediation measures to address the vulnerabilities and cybersecurity gaps identified during the assessment and implement the plan for applying the identified measures.

3. The completed vulnerability assessment form and remediation plan required by this section must be submitted to TSA within 90 days of the effective date of this Security Directive.[6] The required information must be submitted via email to TSA at SurfOpsRail-SD@tsa.dhs.gov, using appropriate methods to protect any Sensitive Security Information contained in the completed assessment and the remediation plan.

PROCEDURES FOR SECURITY DIRECTIVES

A. Owner/Operators must:

1. Immediately provide written confirmation of receipt of this Security Directive via email to TSA at SurfOpsRail-SD@tsa.dhs.gov.

2. Immediately disseminate the information and measures in this Security Directive to corporate senior management, security management representatives, and any personnel having responsibilities in implementing the provisions in this Security Directive.

3. Brief all individuals responsible for implementing this Security Directive.

B. Owner/Operators must share this Security Directive with persons that may be subject to the requirements of the Directive.

C. Owner/Operators must immediately notify TSA at SurfOpsRail-SD@tsa.dhs.gov, if unable to implement any of the measures in this Security Directive within the required timeframe.

DEFINITIONS

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).

[6] To the extent the Owner/Operator identifies gaps or other vulnerabilities in their implementation of cybersecurity recommendations, the assessment submitted to TSA and CISA will be Sensitive Security Information and must be protected according to the requirements in 49 CFR part 1520.

B. *Days* means calendar days unless otherwise indicated.

C. *Information Technology System* means any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of the Owner/Operator to operate and/or maintain.

D. *Operational disruption* means a deviation from or interruption of normal activities or operations that results in a loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, critical information technology systems

E. *Operational Technology System* is a general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.

F. *Unauthorized Access of an Information Technology or Operational Technology System* means access from an unknown or unauthorized source, whether external or internal; access by a third party or former employee; an employee accessing systems for which he or she is not authorized; and may include a non-malicious violation of the Owner/Operators policies, such as the use of shared credential by an employee otherwise authorized to access the system.

APPROVAL OF ALTERNATIVE MEASURES

Owner/Operators must immediately notify TSA via email at TSA-Surface-Cyber@tsa.dhs.gov if unable to implement any of the measures in this Security Directive. Owner/Operators may submit proposed alternative measures and the basis for submitting the alternative measures to TSA for approval to the email address above.

David P. Pekoske
Administrator