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

INFORMATION CIRCULAR

NUMBER Surface Transportation IC-2021-01

SUBJECT Enhancing Surface Transportation Cybersecurity

EFFECTIVE DATE December 31, 2021

EXPIRATION DATE Indefinite

APPLICABILITY This Information Circular applies to the following owner/operators not specifically covered under Security Directives 1580-21-01 or 1582-21-02:

- Each railroad owner/operator identified in 49 CFR 1580.1(a)
- Each passenger railroad, public transportation agency, or rail transit system owner/operator identified in 49 CFR 1582.1
- Each Over-The-Road-Bus owner/operator identified in 49 CFR 1584.1

LOCATION All locations within the United States

SUPERSEDES N/A

PURPOSE AND GENERAL INFORMATION

The United States has a vital national interest in protecting its people and infrastructure from threats in the surface transportation domain. Technologically sophisticated adversaries have demonstrated the ability and continuing desire to mount cyber-attacks to exploit vulnerabilities and to adapt to changes in surface transportation security measures by conducting multiple, simultaneous attacks against the U.S. and its global interests. Cyberattacks against transportation infrastructure are a growing and emerging threat due to the prevalence of remote and anonymous connectivity to a system or network, and the capability to affect a physical consequence through virtual means. *See National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021).

Cybersecurity threats to the surface transportation domain are a persistent and ever evolving threat as the industry continues its dependence on the convenience, efficiencies, connectivity, and the converging of information and operational technology systems. Railroads, public transportation agencies, and over-the-road bus operators all have technology that needs to be appropriately secured. Cyberattacks across all sectors, including transportation, have shown that information and operational technology systems are vulnerable. The recommendations identified below can be applied to improve cybersecurity practices and defenses.

This Information Circular provides recommendations for enhancing cybersecurity practices. First, it recommends the designation of a Cybersecurity Coordinator who would be available to TSA and Cybersecurity and Infrastructure Security Agency (CISA) at all times (all hours/all days) to coordinate implementation of cybersecurity practices, manage security incidents, and serve as a principal point of contact with TSA and CISA for cybersecurity-related matters. Second, it recommends reporting cybersecurity incidents to CISA. Third, it recommends the development of a Cybersecurity Incident Response Plan to reduce the risk of operational disruption should information and/or operational technology systems be affected by a cybersecurity incident. Finally, it recommends conducting cybersecurity vulnerability assessment using the form provided by TSA. The vulnerability assessment includes 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.

While this document is guidance and does not impose requirements on any person or company, TSA most strongly recommends the adoption of the measures herein. The term “should” means that TSA recommends the actions described. Nothing in this document shall supersede federal statutory or regulatory requirements.

RECOMMENDED MEASURES

A. Cybersecurity Coordinator

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

2. Owner/Operators should 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) as soon as practicable or when there is a change in any of the information suggested by this section.

3. The Cybersecurity Coordinator and alternate should—

   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 the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (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 should report to CISA all cybersecurity incidents 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

    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 systems or facilities, or an incident that has the potential to cause impact to a large number of customers, critical infrastructure, or core government functions, or impact to national security, economic security, or public health and safety.

2. Owner/Operators should report the incidents suggested by Section B as soon as practicable, but no later than 24 hours after a cybersecurity incident is identified.

3. Reports should 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.[1] All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

4. The report to CISA should include the following information as available to the reporting owner/operator at the time of the report:

    a. The name of the reporting individual and contact information, including a telephone number or email address.

    b. The affected surface mode, and route(s), facilities, and/or conveyances as applicable.

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

[1] 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 Owner/Operators should report pursuant to this IC as well as the ability to conduct improved analysis.

i. Earliest known date of the 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/Operator, 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 should 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 should submit an initial report within the specified timeframe and supplement as additional information becomes available.

C. Implementing a Cybersecurity Incident Response Plan

1. As soon as practicable, Owner/Operators should 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, should their mode of transportation experience a cybersecurity incident. The Cybersecurity Incident Response Plan should provide specific measures sufficient to ensure the following objectives are achieved, 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 outside of the production environment, 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 should, 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 should conduct annual situational exercises to test the effectiveness of procedures, and personnel responsible for implementing measures, in the Cybersecurity Incident Response Plan.

D. Cybersecurity Vulnerability Assessment

1. Owner/Operators should complete a cybersecurity vulnerability assessment and identification of 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 should identify remediation measures to address the vulnerabilities and cybersecurity gaps identified during the assessment and implement the plan for applying the identified measures.

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).

B. *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.

C. *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

D. *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.

E. *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 freight railroad carrier’s policies, such as the use of shared credential by an employee otherwise authorized to access the system.

Eddie D. Mayenschein
Assistant Administrator
Policy, Plans, and Engagement

APPENDIX A

Additional mitigation guidance and recommended practices are publicly available. The list below is not all inclusive, but represent other references available to use in the development of a cybersecurity self-assessment:

- CISA cybersecurity tips regarding common security issues: https://us-cert.cisa.gov/ncas/tips
- CISA "Recommended Practice: Defense in Depth": https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- NIST Framework for Improving Critical Infrastructure Cybersecurity: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
    - Online NIST Framework self-assessment tool (developed by Department of Energy): https://facilitycyber.labworks.org/assessments/fcf1.1
- NIST 800-82 "Guide to Industrial Control Systems (ICS) Security": https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- NIST 800-53 "Security and Privacy Controls for Information Systems and Organizations": https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- NIST 7621 "Small Business Information Security: The Fundamentals": https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final