



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

MEMORANDUM

To: Covered Railroad Owner/Operators

Date: October 18, 2022

Subject: Issuance of Security Directive (SD) 1580/82-2022-01 and revisions to the SD 1580-21-01 series and the SD 1582-21-01 series.

Attached to this memorandum are SD 1580/82-2022-01, *Rail Cybersecurity Mitigation Actions and Testing*, and revisions to the SD 1580-21-01A series, *Enhancing Rail Cybersecurity*, and SD 1582-21-01A series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*. These SDs take effect on October 24, 2022.

With issuance of SD 1580/82-2022-01, which complements those issued in 2021, TSA recognizes the railroad industry's commitment to strong cybersecurity measures while ensuring a baseline of cybersecurity mitigation measures to protect against current and evolving threats and adversarial capabilities. SD 1580/82-2022-01 applies to each freight railroad carrier identified in 49 CFR 1580.101 and other specific railroad Owner/Operators notified by TSA.

In imposing the requirements in SD 1580/82-2022-01, TSA is committed to providing flexibility in the implementation of security measures to achieve required security outcomes. This SD specifically requires that TSA-designated railroad Owners/Operators implement the following cybersecurity measures to prevent disruptions to their infrastructure:

1. Develop and implement a Cybersecurity Implementation Plan that describes the specific measures employed and the schedule for achieving the outcomes described in Section III.A through III.E of the SD.
2. Establish a Cybersecurity Assessment Program and submit an annual plan to TSA that describes how the Owner/Operator will regularly assess the effectiveness of cybersecurity measures, and identify and resolve device, network, and/or system vulnerabilities.

The SD requires Owner/Operators to submit their Cybersecurity Implementation Plan for TSA approval. This plan, once approved, will be the primary document against which TSA will inspect for compliance with this SD. Owner/Operators are required to provide documentation and access to TSA as necessary to establish compliance.

As noted above, the previously issued SD 1580-21-01 and SD 1582-21-01 series are still in effect. In parallel with the proposed new SD 1580/82-2022-01, TSA is also amending these SDs with the following revisions. First, TSA expanded the applicability of the SD 1580-21-01 series to align with the applicability of SD 1580/82-2022-01. This expanded applicability includes railroads that support the Strategic Rail Corridor Network (STRACNET). Second, TSA is

extending the expiration dates of these SDs from December 31, 2022, to October 24, 2023. Third, the SDs issued to rail Owner/Operators in 2021 included a requirement to develop a Cybersecurity Incident Response Plan by a specific date. While that date has passed, it is critical that rail Owner/Operators maintain and regularly update their Cybersecurity Incident Response Plans. To address this concern, the amendments make the response plans an ongoing requirement for those currently subject to the SDs. For Owner/Operators within the expanded applicability, the SD provides 180-days to complete their Cybersecurity Incident Response Plan.

Although TSA has not designated these three SDs as Sensitive Security Information (SSI), the information submitted to TSA as a result of these requirements is protected as SSI per 49 CFR parts 15 and 1520. The SD requires that Owner/Operators immediately provide written confirmation of receipt of these SDs via email to SurfOps-SD@tsa.dhs.gov. All queries concerning the attached SDs should be submitted to TSA at TSA-Surface@tsa.dhs.gov.

TSA is appreciative of the continued commitment from freight rail owner/operators in the mission to secure the nation's critical railroad infrastructure.



David P. Pecoske
Administrator

Attachments:

- SD 1580/82-2022-01
- SD 1580-21-01A
- SD 1582-21-01A



<u>NUMBER</u>	Security Directive 1580/82-2022-01
<u>SUBJECT</u>	Rail Cybersecurity Mitigation Actions and Testing
<u>EFFECTIVE DATE</u>	October 24, 2022
<u>EXPIRATION DATE</u>	October 24, 2023
<u>SUPERSEDES</u>	Not Applicable
<u>APPLICABILITY</u>	Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads
<u>AUTHORITY</u>	49 U.S.C. 114(d), (f), (l) and (m)
<u>LOCATION</u>	All locations within the United States

I. 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 mitigate 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.”¹

This Security Directive requires actions necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation’s railroads.² Even minor disruptions in critical rail systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply

¹ See *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021).

² This Security Directive is issued under the authority of 49 U.S.C. 114(l)(2)(A), which 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.”

chain disruptions, with ripple effects across the economy. Disruptions and delays may affect industries that depend on the commodities transported by the nation's railroads.

The goal of this Security Directive is to reduce the risk that cybersecurity threats pose to critical railroad operations and facilities through implementation of layered cybersecurity measures that provide defense-in-depth. Recent and evolving intelligence emphasizes the growing sophistication of nefarious persons, organizations, and governments, highlights vulnerabilities, and intensifies the urgency of implementing the requirements of this Security Directive.³

In general, this Security Directive is applicable to the same railroads subject to Security Directive 1580-21-01 "Enhancing Rail Cybersecurity," which first went into effect on December 31, 2021,⁴ and additional TSA-designated freight and passenger railroads notified by TSA based on a risk determination.

To protect against the ongoing threat to the United States' national and economic security, this Security Directive mandates that these railroad Owner/Operators implement the following cybersecurity measures to prevent disruptions to their infrastructure and/or operations. Specifically, Owner/Operators must:

1. Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific measures employed and the schedule for achieving the following outcomes, as more fully described in Section III.A through III.E.:
 - a. Implement network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised;
 - b. Implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems;
 - c. Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and
 - d. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on Critical Cyber Systems in a timely manner using a risk-based

³ See Joint Cybersecurity Advisory (AA22-110A), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (dated April 20, 2022), available at https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf. See also additional information regarding current threats posted at <https://www.cisa.gov/shields-up>.

⁴ Section II.A for applicability.

methodology.

2. Establish a Cybersecurity Assessment Program and submit an annual plan to TSA that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures, and identify and resolve device, network, and/or system vulnerabilities. *See* Section III.F.

The Security Directive requires Owner/Operators to submit a Cybersecurity Implementation Plan for TSA approval. This plan, once approved by TSA, will set the security measures and requirements against which TSA will inspect for compliance.⁵ *See* Section II.B. Owner/Operators are required to provide additional documentation and access to TSA as necessary to establish compliance. *See* Section IV.⁶ In developing their Cybersecurity Implementation Plan, Owner/Operators may use previous risk or vulnerability assessments to assist in identifying Critical Cyber Systems and the prioritization of cybersecurity measures associated with this Security Directive. *See* Section IV.A.

All information that must be reported or submitted to TSA pursuant to this Security Directive is Sensitive Security Information subject to the protections of part 1520 of title 49, Code of Federal Regulations. The Department of Homeland Security may use the information, with company-specific data redacted, for Department of Homeland Security's intelligence-derived reports. TSA and the Cybersecurity and Infrastructure Security Agency also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.⁷ Information provided to Department of Homeland Security pursuant to this Security Directive may also be shared with other agencies as appropriate.⁸ The distribution, disclosure, and availability of information will be restricted to persons with a need to know, and safeguarding, protecting, and marking methods for sensitive/critical information will be utilized.⁹ As required, TSA sought approval from the Office of Management and Budget for a revision to Office of Management and Budget Control No. 1652-0074 for the collection of information under this Security Directive.

TSA is issuing this Security Directive in consultation with the Cybersecurity and Infrastructure Security Agency, the Department of Defense, and the Department of Transportation. TSA will seek review and ratification of this Security Directive by the Transportation Security Oversight Board. The Transportation Security Oversight Board is

⁵ *See also* 49 U.S.C. 114(f); 49 CFR part 1503.

⁶ *See also* 49 U.S.C. 114(f).

⁷ *See* OMB Control No. 1670-0037.

⁸ Presidential Policy Directive (PPD) 41 requires Federal agencies to rapidly share incident information with each other to achieve unity of governmental effort. *See* PPD-41 § III.D ("Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident"). Furthermore, for purposes of information shared with the Department of Homeland Security pursuant to this directive, cyber incident responders with responsibilities under PPD-41 are "covered" persons with a "need to know," as provided by 49 CFR 1520.7 and 1520.11, respectively.

⁹ *See* 49 CFR 1520.5(b)(5) and <https://www.tsa.gov/for-industry/sensitive-security-information>.

statutorily required to “review and ratify or disapprove” emergency regulations and security directives issued by TSA under 49 U.S.C. 114(l)(2). *See* 49 U.S.C. 114(l)(2)(B) and 115(c)(1). If, for whatever reason, the Transportation Security Oversight Board fails to ratify any section or subsection of this Security Directive, or deems any section or subsection inapplicable, the remainder of this Security Directive shall not be affected.

II. ACTIONS REQUIRED

A. Applicability, Deadlines for Compliance, and Scope

1. *Applicability*: The provisions of this Security Directive apply to the following Owner/Operators:
 - a. Freight Railroad Owner/Operators subject to applicability described in 49 CFR 1580.101.
 - b. *Other TSA-designated Freight and Passenger Railroad Owner/Operators*: This Security Directive also applies to Owner/Operators of railroads designated by TSA. TSA will notify these Owner/Operator(s) and provide specific compliance deadlines for the requirements in this Security Directive.
2. *Scope*: The requirements in this Security Directive apply to Critical Cyber Systems of TSA-designated freight and passenger railroads.

Note: If an Owner/Operator determines they have no Critical Cyber Systems, as defined in Section VII of this Security Directive, they must notify TSA in writing within 60 days of the effective date of this Security Directive. In the event that an Owner/Operator’s method of operation changes, they must reevaluate whether they have a Critical Cyber System, and if so, the requirements of this Security Directive are applicable.

B. Cybersecurity Implementation Plan

1. No later than 120 days after the effective date of this Security Directive, Owner/Operators must submit a Cybersecurity Implementation Plan to SurfOps-SD@tsa.dhs.gov for TSA approval.
2. The Cybersecurity Implementation Plan must provide all the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the Owner/Operator’s defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.
3. Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan in accordance with the schedule as stipulated in the plan.

III. CYBERSECURITY MEASURES

The Owner/Operator must:

- A. Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII of this Security Directive.
- B. Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice-versa. As applied to Critical Cyber Systems, these policies and controls must include:
 1. A list and description of —
 - a. Information Technology and Operational Technology system interdependencies;
 - b. All external connections to the Information Technology and Operational Technology system;
 - c. Zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity; and
 - d. Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.
 2. An identification and description of measures for securing and defending zone boundaries, that includes security controls—
 - a. To prevent unauthorized communications between zones; and
 - b. To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.
- C. Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. These measures must incorporate the following policies, procedures, and controls:
 1. Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include—

- a. A policy for memorized secret authenticators resets that includes criteria for when resets must occur¹⁰; and
 - b. Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (III.C.1.a), and a timeframe to complete these mitigations.
2. Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.
 3. Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.
 4. Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure—
 - a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and
 - b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.
 5. Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.
- D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:
1. Capabilities to—
 - a. Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;

¹⁰ This policy should be compliant with the most current version of the National Institute of Standards and Technology's Special Publication 800-63, Digital Identity Guidelines (available at <https://csrc.nist.gov/publications/detail/sp/800-63/3/final>).

- b. Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;
 - c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;
 - d. Block and prevent unauthorized code, including macro scripts, from executing; and
 - e. Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).
2. Procedures to—
- a. Audit unauthorized access to internet domains and addresses;
 - b. Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;
 - c. Identify and respond to execution of unauthorized code, including macro scripts; and
 - d. Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.
3. Logging policies that –
- a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and
 - b. Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.
4. Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.¹¹
- E. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical

¹¹ See related requirement in section C.1.a. in the SD 1580-21-01 series.

Cyber Systems consistent with the Owner/Operator's risk based methodology. These measures must include:

1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.
 2. The strategy required by section III.E.1. must include:
 - a. The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and
 - b. Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.¹²
 3. If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability to meet necessary capacity, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.
- F. Develop a Cybersecurity Assessment Program for proactively assessing and auditing cybersecurity measures.
1. The Owner/Operator must develop a Cybersecurity Assessment Program for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.
 2. The Cybersecurity Assessment Program required by Section III.F.1. must –
 - a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;
 - b. Include an architectural design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. An architectural design review contains verification and validation of network traffic, a system log review, and analysis to identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems; and
 - c. Incorporate other assessment capabilities designed to identify vulnerabilities based on evolving threat information and adversarial capabilities, such as

¹² Available at: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

penetration testing of Information Technology systems, including the use of “red” and “purple” team (adversarial perspective) testing.

3. No later than 60 days after TSA’s approval of the Owner/Operator’s Cybersecurity Implementation Plan, the Owner/Operator must submit the annual plan for their Cybersecurity Assessment Program to SurfOps-SD@tsa.dhs.gov. This plan must describe the Cybersecurity Assessment Program required by Section III.F.1, including the schedule for specific actions. The Owner/Operator must update this plan on an annual basis and submit it no later than one year from the date of the previous plan’s submission.

IV. RECORDS

- A. *Use of previous plans, assessments, tests, and evaluations.* As applicable, Owner/Operators may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this Security Directive. If the Owner/Operator relies on these materials, they must include an index of the records and their location organized in the same sequence as the requirements in this Security Directive.
- B. *Protection of sensitive security information.* The Owner/Operator must, at a minimum, store and transmit the following information required by this Security Directive consistent with the requirements in 49 CFR part 1520:¹³
 1. Plans and reports; and
 2. Audit, testing, or assessment results.
- C. *Documentation to Establish Compliance*
 1. The Owner/Operator must make records necessary to establish compliance with this Security Directive available to TSA upon request for inspection and/or copying.
 2. TSA may request to inspect or copy the following documents to establish compliance with this Security Directive:
 - a. Hardware/software asset inventory, including supervisory control, and data acquisition systems;
 - b. Firewall rules;

¹³ Owner/Operators may contact SSI@tsa.dhs.gov for more information on how to comply with requirements for the protection of Sensitive Security Information.

- c. Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks.
- d. Policy, procedural, and other documents that informed the development, and documented implementation of, the Owner/Operator's Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, Cybersecurity Assessment Program, and assessment or audit results.
- e. Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as –
 - i. Log files;
 - ii. A capture of network traffic (e.g., packet capture (PCAP)), not to exceed a period of twenty-four hours, as identified and directed by TSA;
 - iii. "East-West Traffic" of Operational Technology systems/sites/environments within the scope of this Security Directive's requirements; and
 - iv. "North-South Traffic" between Information and Operational Technology systems, and the perimeter boundaries between them.
- f. Any other records or documents necessary to establish compliance with this Security Directive.

V. PROCEDURES FOR SECURITY DIRECTIVES

A. General Procedures

1. *Confirm Receipt.* Immediately provide written confirmation of receipt of this Security Directive via e-mail to SurfOps-SD@tsa.dhs.gov;
2. *Dissemination.* Immediately disseminate the information and measures in this Security Directive to corporate senior management and security management representatives. The Owner/Operator must provide the applicable security measures in this Security Directive to the Owner/Operator's direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.

- B. *Comments.* Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this Security Directive must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive or requirement to comply with the provisions of the Security Directive.

VI. AMENDMENTS TO CYBERSECURITY IMPLEMENTATION PLAN

- A. *Changes to ownership or control of operations.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, there are any changes to the ownership or control of the operation.
- B. *Changes to conditions affecting security.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, the Owner/Operator makes, or intends to make, permanent changes to the policies, procedures, or measures approved by TSA, including, but not limited to changes to address:
1. Determinations that a specific policy, procedure, or measure in the Cybersecurity Implementation Plan is ineffective based on results of the audits and assessments required under Section III.F. of this Security Directive; or
 2. The Owner/Operator has identified or acquired new or additional Critical Cyber Systems or capabilities for meeting the requirements in the Security Directive that have not been previously approved by TSA.
- C. *Permanent change.* For purposes of this section, a “permanent change” is one intended to be in effect for 45 or more days.
- D. *Schedule for requesting amendment.* The Owner/Operator must file the request for an amendment to its Cybersecurity Implementation Plan with TSA no later than 50 days after the permanent change takes effect, unless TSA allows a longer time period.
- E. *TSA approval.*
1. TSA may approve a requested amendment to a Cybersecurity Implementation Plan if TSA determines that it is in the interest of public and transportation security and the proposed amendment provides the level of security required under this Security Directive.
 2. TSA may request additional information from the Owner/Operator before rendering a decision.
- F. *Petition for reconsideration.* No later than 30 days after receiving a denial of an amendment to a Cybersecurity Implementation Plan, the Owner/Operator may file a petition for reconsideration following the procedures set in 49 CFR 1570.119.


VII. DEFINITIONS

In addition to the terms defined in 49 CFR 1500.3, 1570.3 and Security Directives 1580-21-01 and 1582-21-01, the following terms apply to this Security Directive:

- A. *Critical Cyber System* means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include those business services that, if compromised or exploited, could result in operational disruption.
- B. *Cybersecurity Architecture Design Review* means a technical assessment based on government and industry-recognized standards, guidelines, and best practices that evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews must be designed to be applicable to the Owner/Operator's Information and Operational Technology systems.
- C. *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).
- D. *Days* means calendar days unless otherwise indicated. As used for compliance deadlines, if a requirement must be met on a date that is a national holiday, the compliance deadline will be the next federal business day after the holiday.
- E. *East-West traffic* means, in a networking context, the lateral movement of network traffic within a trust zone or local area network.
- F. *Group policy* means a centralized place for administrators to manage and configure operating systems, applications and users' settings that can be used to increase the security of users' computers and help defend against both insider threats and external attacks.
- G. *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 maintain.
- H. *Interdependencies* means relationships of reliance within and among Information and Operational Technology systems that must be maintained for those systems to operate and provide services.

- I. *Memorized secret authenticator* means a type of authenticator comprised of a character string intended to be memorized by, or memorable to, the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process
- J. *Necessary capacity* means the Owner/Operator's determination of capacity to support their business critical functions required for railroad operations and supply chain expectations.
- K. *North-South traffic* means network traffic that moves through a perimeter boundary into another trust level.
- L. *Operational disruption*, for purposes of this Security Directive, means a deviation from or interruption of necessary capacity that results from a compromise or loss of data, system availability, system reliability, or control of a railroad subject to this Security Directive.
- M. *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.
- N. *Owner/Operator* means a railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.
- O. *Phishing* means tricking individuals into disclosing sensitive personal information through deceptive computer-based means such as internet web sites or e-mails using social engineering or counterfeit identifying information.
- P. *Security, Orchestration, Automation, and Response (SOAR)* means capabilities that enable Owner/Operators to collect inputs monitored by the security operations team. For example, alerts from the security information and event management system and other security technologies – where incident analysis and triage can be performed by leveraging a combination of human and machine power – help define, prioritize and drive standardized incident response activities. These capabilities allow an Owner/Operator to define incident analysis and response procedures in a digital workflow format.
- Q. *Shared account* means an account that is used by multiple users with a common authenticator to access systems or data. A shared account is distinct from a group account, which is a collection of user accounts that allows administrators to group similar user accounts together in order to grant them the same rights and permissions. Group accounts do not have common authenticators.

- R. *Spam* means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- S. *Tor*, also known as The Onion Router, means software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. Tor software obfuscates a user's identity from anyone seeking to monitor online activity (such as nation states, surveillance organizations, information security tools). This deception is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol address of a Tor exit node, as opposed to the address of the user's computer.
- T. *Trust relationship* means an agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets. This term refers to trust relationships between system elements implemented by hardware, firmware, and software.
- U. *Unauthorized access of an Information Technology or Operational Technology system* means access from an unknown source; 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 Owner/Operator policy violation such as the use of a shared credential by an employee otherwise authorized to access it.



David P. Pekoske
Administrator



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

<u>NUMBER</u>	Security Directive 1580-21-01A
<u>SUBJECT</u>	Enhancing Rail Cybersecurity
<u>EFFECTIVE DATE</u>	October 24, 2022
<u>EXPIRATION DATE</u>	October 24, 2023
<u>CANCELS AND SUPERSEDES</u>	Security Directive 1580-21-01
<u>APPLICABILITY</u>	Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight railroads
<u>AUTHORITY</u>	49 U.S.C. 114(d), (f), (l) and (m)
<u>LOCATION</u>	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 applies to all freight railroad carriers (Owner/Operators) described in 49 CFR 1580.101 and other TSA-designated freight railroads and requires four critical actions:

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;

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. 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.²

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.³ 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 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

² 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.

³ 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.

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 freight railroad carrier'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 customers or passengers (as applicable), 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) 282-0870.⁴ 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 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.

⁴ 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.

- 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. Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for their Critical Cyber Systems, as defined in SD 1580/82-22-02 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. Owner/Operators who were not previously required to develop and adopt a Cybersecurity Incident Response Plan must complete their plan within 180-days of the effective date of this SD. Within 7 days of completing their plan, the Owner/Operator 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.⁵ 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).
- 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.

⁵ 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.

- 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



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

NUMBER Security Directive 1582-21-01A

SUBJECT Enhancing Public Transportation and Passenger Railroad Cybersecurity

EFFECTIVE DATE October 24, 2022

EXPIRATION DATE October 24, 2023

CANCELS AND SUPERSEDES Security Directive 1582-21-01

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 system² 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. Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan for their Critical Cyber Systems, as defined in SD 1580/82-22-02, 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.

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

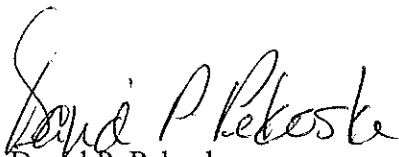
- A. *Cybersecurity incident* means an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, 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).
- 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.

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.

- 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. Pecoske
Administrator