U.S. DEPARTMENT OF HOMELAND SECURITY TRANSPORTATION SECURITY ADMINISTRATION (TSA)	**Cybersecurity Measures for Surface Modes** **Surface Transportation Information Circular (IC)-2021-01 and IC Surface-2025-01**	**OMB No. 1652-0074** **Exp: 8/31/2026**

Who must comply?	Surface Transportation IC-2021-01: • Owner/Operators not specifically covered by the Security Directive (SD) 1580-26-02 series,[1] including railroad, passenger railroad, public transportation agency, rail transit system, and Over-The-Road Bus (OTRB) operations. IC Surface-2025-01: • Owner/Operators covered by the below security directive series and those required to report significant security concerns to TSA under the below authority.
What is this information collection about?	TSA provides recommendations to enhance surface transportation cybersecurity and reduce the risk of operational disruption through layered cybersecurity measures. In order to implement cybersecurity practices to help protect transportation infrastructures and operations across railroad, public transportation, pipeline, and OTRB systems, Owner/Operators should: Surface Transportation IC-2021-01: • Designate a primary and at least one alternate Cybersecurity Coordinator and one or more alternate(s) who is available to TSA 24 hours a day, 7 days a week, to coordinate cybersecurity and related practices and address any incidents that arise; • Report cybersecurity incidents to CISA as soon as practicable, but no later than 24 hours after identification by the Owner/Operator (see below for how to report); • Develop a Cybersecurity Incident Response Plan that includes measures to reduce the risk of operational disruption should Information and/or Operational Technology systems be affected by a cybersecurity incident and conduct situational exercises to test the effectiveness of the procedures and personnel responsible for implementing the measures; and • Conduct a cybersecurity vulnerability assessment using the TSA-issued form and submit the completed form to TSA. IC Surface-2025-01:

[1] Consolidated SD 1580-21-01 series; SD 1582-21-01 series; and SD Pipeline 2021-01 series

	• Notify TSA's Transportation Security Operations Center (TSOC) as soon as possible, and no more than 12 hours after discovery of an actual or potential significant cybersecurity incident.
Where do I find the requirements for this information collection?	Surface Transportation IC-2021-01: • 49 CFR § 1580.1 (a) • 49 CFR § 1582.1 • 49 CFR § 1584.1 IC Surface-2025-01: • 49 CFR § 1570.203 • SD 1580-26-02 series
When must information be submitted to TSA and CISA?	Surface Transportation IC-2021-01: • TSA submission dates will vary and Owner/Operators are encouraged to contact their local TSA representative. • Owner/Operators should report cybersecurity incidents to CISA as soon as practicable, but no later than 24 hours after an incident has been identified. IC Surface-2025-01: • Owner/Operators should notify TSA's TSOC as soon as possible, and no more than 12 hours after discovery of an actual or potential significant cybersecurity incident.
How must documents and information be submitted?	Surface Transportation IC-2021-01: • Email TSA TSA-Surface-Cyber@tsa.dhs.gov. • Cybersecurity incidents should be made to CISA Central using CISA's Incident Reporting System at: https://myservices.cisa.gov/irf or by calling (844) 729-2472. IC Surface-2025-01: • Owner/Operators should notify TSA's TSOC via telephone (1-866-655-7023).
How does TSA use the information received?	Surface Transportation IC-2021-01 • Information collected is securely stored in a protected database and shared with TSOC to support operational needs. Additionally, contact details for Cybersecurity Coordinators are used to facilitate the exchange of cybersecurity-related information and communication with TSA and CISA.

For additional information, contact--	TSA-Surface-Cyber@tsa.dhs.gov

PAPERWORK REDUCTION ACT (PRA) STATEMENT:
Statement of Public Burden: This is a voluntary collection of information. TSA estimates that the total annual burden associated with this information collection for Owner/Operators under the recommendations in Surface Transportation IC-2021-01 and IC Surface-2025-01 is approximately 0.083 hours to designate a Cybersecurity Coordinator; 20 hours for the Cybersecurity Incident Response Plan updates; 42 hours for the Cybersecurity Vulnerability Assessment; and 0.33 hours for reporting cybersecurity incidents. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The control number for this collection is OMB Control No. 1652-0074, which expires 8/31/2026. Send comments regarding this burden estimate or any other aspect of this collection of information including suggestions for reducing this burden to TSAPRA@tsa.dhs.gov or TSA, TSA-11, 6595 Springfield Center Drive, Springfield, VA 20598-6011. ATTN: PRA 1652-0074 *Cybersecurity Measures for Surface Modes*.