

U.S. DEPARTMENT OF HOMELAND SECURITY TRANSPORTATION SECURITY ADMINISTRATION (TSA)	Cybersecurity Measures for Surface Modes Security Directive series 1580-21-01 1582-21-01	OMB No. 1652-0074 Exp: 8/31/2026
--	--	---

Who must comply?	Freight railroad carriers, passenger railroad carriers or rail transit systems, and other TSA-designated railroads covered by the Security Directive (SD) 1580-21-01 series and the SD 1582-21-01 series.
What is this information collection about?	TSA is requiring Owners/Operators of each freight railroad carrier, passenger railroad carrier or rail transit system, and other TSA-designated railroads to implement cybersecurity measures 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. The requirements include the following: • 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; • Ensure any non-U.S. citizen serving as a primary or alternate Cybersecurity Coordinator is a current member of NEXUS, Global Entry, or another program determined by TSA to include a comparable security threat assessment and submit documentation of such membership to TSA; • Report cybersecurity incidents to CISA no later than 72 hours after identification by the Owner/Operator (see below for how to report); • Develop and maintain 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 • For newly designated owner/operators, conduct a cybersecurity vulnerability assessment using the TSA-issued form and submit the completed form to TSA. TSA expects fewer than 10 new Owner/Operators will need to submit this assessment annually.
Where do I find the requirements for this	Authorities: 49 U.S.C. 114(d), (f), (l), and (m). 49 CFR § 1580.101; § 1582.101.

information collection?	SD Series: SD 1580-21-01 (Sections II.B., II.C., II.D., II.E). SD 1582-21-01 (Sections II.B., II.C., II.D., II.E).
When must information be submitted to TSA and CISA?	TSA - Submission dates will vary and Owner/Operators are encouraged to contact their local TSA representative. CISA - Owner/Operators must report cybersecurity incidents to CISA, as soon as practicable, but no later than 72 hours after the Owner/Operator identifies a cybersecurity incident.
How must documents and information be submitted?	TSA - Email at SurfOpsRail-SD@tsa.dhs.gov. - Upload at TSA Secure Regulatory Portal. - Retain locally for in-person or other review pursuant to TSA-approved methods, which may include virtual review. CISA - Cybersecurity incidents must be made to CISA Central using CISA's Incident Reporting System at: http://www.cisa.gov/report or by calling (844) 729-2472.
How does TSA use the information received?	TSA 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 mandatory collection of information. TSA estimates that the total annual burden associated with this information collection for Owner/Operators subject to the SD 1580-21-01 series and the SD 1582-21-01 series is approximately 0.083 hours to Designate a Cybersecurity Coordinator ; 1.48 hours for STA; 20 hours for the Cybersecurity Incident Response Plan updates; 42 hours for the Cybersecurity Vulnerability Assessment form, 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*.