U.S. DEPARTMENT OF HOMELAND SECURITY TRANSPORTATION SECURITY ADMINISTRATION (TSA)	**Cybersecurity Measures for Surface Modes** Security Directive series 1580/82-2022-01	**OMB No. 1652-0074** **Exp: 8/31/2026**

Who must comply?	Freight railroad carriers and other TSA-designated freight and passenger railroads covered by the Security Directive (SD) 1580/82-2022-01 series.
What is this information collection about?	TSA is requiring Owner/Operators of freight railroad carriers and other TSA-designated freight and passenger 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: • Establish and implement a TSA-approved Cybersecurity Implementation Plan that identifies how the Owner/Operator will achieve each of the objectives in the security directive; • Develop and maintain a Cybersecurity Assessment Plan 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. Owner/Operators must also submit an annual report that provides Cybersecurity Assessment Plan results from the previous year; and • Provide documentation to TSA upon request as necessary to establish compliance.
Where do I find the requirements for this information collection?	Authorities: 49 U.S.C. 114(d), (f), (*l*)**,** and (m); 49 CFR § 1580.101. SD Series: SD 1580-2022-01 (Sections II.B. and III.F.).
When must information be submitted to TSA?	Submission dates will vary and Owner/Operators are encouraged to contact their local TSA representative.
How must documents and information be submitted?	• 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
How does TSA use the information received?	Upon receipt of documentation, TSA confirms they have been received and saves them in the Owner/Operator's secure file. An

	inspector reviews the documentation for compliance with the applicable security directives and surface transportation regulations. If changes are needed, TSA may suggest a corrective action plan. TSA then records whether the documents are approved or denied in its tracking system (PARIS) to establish an official record.
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 1580/82-2022-01 series is approximately 15 hours for the Cybersecurity Implementation Plan/update, 160 hours for the Cybersecurity Assessment Plan, 120 hours for the annual Cybersecurity Assessment Plan report, and 80 hours for compliance documentation. 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*.