[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Revision of Agency Information Collection Activity Under OMB Review: Cybersecurity Measures for Surface Modes

AGENCY: Transportation Security Administration, DHS.

ACTION: 30-day notice.

SUMMARY: This notice announces that the Transportation Security Administration (TSA) has forwarded the Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652-0074, abstracted below, to OMB for a revision of the currently approved collection under the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. The collection involves the designation of a Cybersecurity Coordinator; the reporting of cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency; the development of a cybersecurity contingency/recovery plan to address cybersecurity gaps; and the completion of a cybersecurity assessment.

DATES: Send your comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. A comment to OMB is most effective if OMB receives it within 30 days of publication.

ADDRESSES: Written comments and recommendations for the proposed information collection should be sent within 30 days of publication of this notice to www.reginfo.gov/public/do/PRAMain. Find this particular information collection by selecting "Currently under Review - Open for Public Comments" and by using the find function.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh, TSA PRA Officer, Information Technology, TSA-11, Transportation Security Administration, 6595

Springfield Center Drive, Springfield, VA 20598-6011; telephone (571) 227-2062; e-mail TSAPRA@tsa.dhs.gov.

SUPPLEMENTARY INFORMATION:

TSA published a *Federal Register* notice, with a 60-day comment period soliciting comments, of the following collection of information on April 16, 2026, 91 FR 20475.

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*), 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 ICR documentation will be available at https://www.reginfo.gov upon its submission to OMB. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to—

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

Title: Cybersecurity Measures for Surface Modes.

Type of Request: Revision.

OMB Control Number: 1652-0074.

Form(s): TSA Optional Forms.

Affected Public: Owner/Operators with operations identified in 49 CFR part 1580 (Freight Rail), 49 CFR part 1582 (Mass Transit and Passenger Rail), and 49 CFR part 1584 (Over-the-Road Bus).

Abstract: Under the authorities of 49 U.S.C. 114, TSA may take immediate action to impose measures to protect transportation security without providing notice or an opportunity for comment.[1] On December 17, 2021, TSA issued the Security Directive (SD) 1580-21-01 series, *Enhancing Rail Cybersecurity,* and the SD 1582-21-01 series, *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, mandating TSA-specified Owner/Operators of higher risk railroads and rail transit systems, respectively, to implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure; these SDs became effective December 31, 2021. In addition, on October 18, 2022, TSA issued the SD 1580/82-2022-01 series, *Rail Cybersecurity Mitigation Actions and Testing*, which applies to Owner/Operators of the "Higher Risk" freight railroads identified in 49 CFR 1580.101 and additional TSA-designated freight and passenger railroads. This SD, which is complementary to the requirements in the previous directives, took effect on October 24, 2022. On December 17, 2021, TSA also issued Information Circular (IC) 2021-01, *Enhancing Surface Transportation Cybersecurity*, which recommended voluntary implementation of actions and reporting by Owner/Operators not covered by the SDs. On October 25, 2025, TSA issued IC Surface-2025-01, *Notifying TSA of Significant Cybersecurity Incidents*, which recommends voluntary reporting of cybersecurity incidents to TSA and Owner/Operators not covered by the SDs.

---

[1] TSA issues SDs for surface transportation operators under the statutory authority of 49 U.S.C. 114(*l*)(2)(A). 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 SD must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or SD without providing notice or an opportunity for comment and without prior approval of the Secretary."

On January 15, 2026, TSA revised the SD 1580-21-01 series, SD 1582-21-01 series, to require that any non-U.S. citizen serving as a primary or alternate Cybersecurity Coordinator must be a current member of NEXUS, Global Entry, or another program determined by TSA to include a comparable security threat assessment. TSA is revising the collection to include this new requirement.

A. SD 1580-21-01 series, SD 1582-21-01 series, Surface Transportation IC-2021-01, and IC Surface-2025-01

These SDs and ICs remain in effect and include the following information collection requirements for the SDs and voluntary collection under the ICs:

1. Designate a primary and at least one alternate Cybersecurity Coordinator; 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. This requirement is a revision to the original collection as discussed above, stemming from the revision of these SD series. TSA expects that fewer than 10 Owner/Operators will respond to the information collection annually. However, this new requirement burden is covered under OMB control number 1651-0121 Trusted Traveler Programs and U.S. APEC Business Travel Card;
2. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency no later than 72 hours after the Owner/Operator identifies a cybersecurity incident;
3. Develop a Cybersecurity Incident Response Plan to TSA; and

4. Complete a cybersecurity vulnerability assessment using the TSA-issued form and submit the completed assessment to TSA.[2]

The collection of information is also being revised to remove mandatory requirements associated with the SD 1580-21-01 series and the SD 1582-21-01 series, specifically the cybersecurity vulnerability assessment for rail Owner/Operators subject to these SDs. These rail Owner/Operators have satisfied these SD requirements and TSA expects that fewer than 10 Owner/Operators will respond to the collection annually.

In addition, TSA is revising the collection to include updates to the Cybersecurity Incident Response Plan requirements. Owner/Operators have developed their initial Cybersecurity Incident Response Plans, satisfying the SD requirements, and TSA expects fewer than 10 new Owner/Operators will need to submit a plan annually. However, TSA also requires these Owner/Operators to maintain up-to-date Cybersecurity Incident Response Plans, which necessitates periodic updates. TSA is revising the collection to include these updates.

IC Surface-2025-01 recommends that Owner/Operators should notify TSA's Transportation Security Operations Center via telephone (1-866-655-7023) as soon as possible, and no more than 12 hours after discovery of an actual or potential significant cybersecurity incident.

B. SD 1580/82-2022-01 Series

This SD series includes the following information collection:

1. Submission of a Cybersecurity Implementation Plan to TSA for approval that identifies how the Owner/Operator will achieve the required security outcomes in the SD;

[2] This is a non-recuring cybersecurity vulnerability assessment. Owner/Operators are required to provide the requested information on a single occasion only.

2. Submission of a Cybersecurity Assessment Plan and submission of an annual Cybersecurity Assessment Plan report; and
3. Documentation provided to TSA upon request as necessary to establish compliance.

The ICs also include the following recommendation but is not a requirement in the SDs: Owner/Operators should notify TSA's Transportation Security Operations Center as soon as possible, and no more than 12 hours after discovery of an actual or potential significant cybersecurity incident.

The collection of information is also being revised to include updates and reports to the mandatory requirements associated with the SD 1580-21-01 series and the SD 1582-21-01 series, specifically the Cybersecurity Implementation Plan and Cybersecurity Assessment Plan for rail Owner/Operators subject to these SDs. These rail Owner/Operators have satisfied the Cybersecurity Implementation Plan requirements and TSA expects fewer than 10 new Owner/Operators will respond to the collection annually. However, TSA estimates that annually about half of Owner/Operators will provide updates to their Cybersecurity Implementation Plan. TSA is revising the collection to include these updates.

In addition, TSA is revising the collection to include updates to the Cybersecurity Incident Response Plan requirements. Owner/Operators have developed their initial Cybersecurity Incident Response Plans, satisfying the SD requirements, and TSA expects fewer than 10 new Owner/Operators will need to submit a plan annually. However, TSA also requires these Owner/Operators to maintain up-to-date Cybersecurity Incident Response Plans, which necessitates periodic updates. TSA is revising the collection to include these updates.

The collection of information is also being revised to include updates and reports to the Cybersecurity Implementation Plan and Cybersecurity Assessment Plan for rail

Owner/Operators subject to these SDs. These rail Owner/Operators have satisfied the Cybersecurity Implementation Plan requirements and TSA expects fewer than 10 new Owner/Operators will respond to the collection annually. However, TSA estimates that annually about half of the Owner/Operators will provide updates to their Cybersecurity Implementation Plan. TSA is revising the collection to include these updates.

In addition, TSA is revising the collection to include Cybersecurity Assessment Plan Reports. In October 2023, SD 1580/82-2022-01 required Owner/Operators to submit an annual report. These Owner/Operators are also required to conduct annual assessments of their cybersecurity measures and submit to TSA an annual report of the results of these assessments. TSA is updating the collection to include these reports.

Portions of the responses that are deemed sensitive security information are protected in accordance with procedures meeting the transmission, handling, and storage requirements of sensitive security information set forth in 49 CFR part 1520.[3]

Estimated Number of Respondents: 67. [4]

Estimated Annual Burden Hours: 22,167.

Dated: August 28, 2026.

Christina A. Walsh,
Paperwork Reduction Act Officer,
Information Technology,
Transportation Security Administration.

[FR Doc. 2026-17894 Filed: 8/28/2026 4:15 pm; Publication Date: 9/1/2026]

[3] In addition, all data in TSA systems are statutorily required to comply with the Federal Information Security Modernization Act 2014 following the National Institute of Standards and Technology Special Publication 800.37 REV2 or Risk Management Framework, and other federal information security requirements including Federal Information Processing Standards 199 and Executive Order 14028. All systems, networks, servers, clouds and endpoints under the Federal Information Security Modernization Act 2014 boundary are hardened to meet the Department of Defense Security Technical Implementation Guidelines, as well as DHS Policy (4300.A) and TSA policy (TSA IA Handbook).

[4] After publishing the 60-day notice, TSA reviewed and updated the number of respondents from 846 to 67 and updated the estimate of the annual time burden from 210,684 hours to 22,167 hours.