[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request a Revision from OMB of One Current Public Collection of Information: Cybersecurity Measures for Surface Modes

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day Notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently-approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652–0074, abstracted below, that we will submit to OMB for a revision in compliance with the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. The collection concerns data concerning 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 60 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: Comments may be e-mailed to TSAPRA@tsa.dhs.gov or delivered to the TSA PRA Officer, Information Technology, TSA-11, Transportation Security Administration, 6595 Springfield Center Drive, Springfield, VA 20598-6011.

FOR FURTHER INFORMATION CONTACT: Christina A. Walsh at the above address, or by telephone (571) 227-2062.

SUPPLEMENTARY INFORMATION:

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

OMB Control Number 1652-0074; Cybersecurity Measures for Surface Modes. TSA is specifically empowered to assess threats to transportation;[1] develop policies, strategies, and plans for dealing with threats to transportation;[2] oversee the implementation and adequacy of security measures at transportation facilities;[3] and carry out other appropriate duties relating to transportation security.[4] Additionally, under 49

[1] 49 U.S.C. 114(f)(2).
[2] 49 U.S.C. 114(f)(3).
[3] 49 U.S.C. 114(f)(11).
[4] 49 U.S.C. 114(f)(15).

U.S.C. § 114(*l*)(2),[5] TSA has the authority to issue Security Directives (SDs) if the Administrator of TSA determines that a regulation or SD must be issued immediately in order to protect transportation security.

On December 17, 2021, TSA issued the 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. The provisions in the directives are reviewed and reissued on an annual basis.

On January 15, 2026, TSA revised the SD 1580-21-01 series and the SD 1582-21-01 series, requiring 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 (STA). TSA is revising the collection to include this new requirement.

[5] 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.

The information collected pursuant to the requirements in the SDs and the recommendations in the IC allow TSA to execute its security responsibilities within the surface transportation industry, through awareness of potential security incidents and suspicious activities. TSA collects the following information:

A. 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 meet the required security outcomes in the SD;
2. Submission of a Cybersecurity Assessment Plan that describes how the Owner/Operator will assess the effectiveness of their cybersecurity measures and an annual report that provides the results of assessments from the previous year;
3. Documentation provided to TSA upon request as necessary to establish compliance.

B. SD 1580-21-01, SD 1582-21-01, Surface Transportation IC-2021-01, and IC Surface-2025-01 Series

The SDs and ICs include the following information collection requirements for the SDs and voluntary collection under the ICs:

1. Provide contact information for a primary and at least one alternate Cybersecurity Coordinator to TSA.
2. Designate any non-U.S. citizen serving as a primary or alternate Cybersecurity Coordinator who is a current member of NEXUS, Global Entry, or another program determined by TSA to include a comparable STA, and submit documentation of such membership to TSA. This requirement is a revision to

the collection as discussed above, stemming from the revision of this surface transportation SD series.

3. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency. Under 49 CFR 1570.203, Owner/Operators must report the incidents required by directives, as soon as practicable, but no later than 72 hours after the Owner/Operator identifies a cybersecurity incident.
4. 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
5. Conduct a cybersecurity vulnerability assessment using the TSA-issued form and submit the completed assessment to TSA.

The IC also includes the following recommendation but is not a requirement in the SDs: 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.

TSA uses the collection of information to ensure compliance with TSA's cybersecurity measures required by the SDs and the recommendations under the ICs.

Owner/Operators can complete and submit the required Cybersecurity Implementation Plans (including any amendments or revisions) and documents incorporated by reference into Cybersecurity Implementation Plans, Cybersecurity Assessment Plans, and related annual reports, using the TSA Secure Regulatory Portal or they may opt to retain documents locally for either in-person or other review pursuant to TSA-approved methods, which may include virtual review. Documentation of compliance must be provided upon request. As the measures in the ICs are voluntary, the ICs do not require Owner/Operators to report on their compliance.

TSA, in conjunction with federal partners such as the Cybersecurity and Infrastructure Security Agency, uses the reports of cybersecurity incidents to evaluate and respond to imminent and evolving cybersecurity incidents and threats as they occur, and as a basis for creating new cybersecurity policy moving forward. This monitoring will allow TSA and federal partners to take action to contain threats, take mitigating action, and issue timely warnings to similarly situated entities against further spread of the threat. TSA and its federal partners also use the information to inform timely modifications to cybersecurity requirements to improve transportation security and national economic security. TSA uses the collection of information to ensure compliance with TSA's cybersecurity measures required by the SDs and the recommendations under the ICs.

Portions of the responses that are deemed Sensitive Security Information (SSI) are protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in 49 CFR part 1520.[6]

TSA estimates SD 1580/82-2022-01 applies to a total of 73 Owner/Operators; and SD 1580-21-01, SD 1582-21-01, and Surface Transportation IC-2021-01 apply to 449 railroad Owner/Operators, 242 public transportation agencies and rail transit system Owner/Operators, and 72 over-the-road bus Owner/Operators, for a total of 836 respondents. TSA estimates the annual hour burden to be 210,661.

In terms of the revision to include the STA requirement, TSA anticipates that only nine or fewer Owner/Operators will need to respond annually to the STA requirement for a non-U.S. citizen to be designated as Cybersecurity Coordinator. However, the burden scope estimates presume that 10 or more Owner/Operators could respond. TSA estimates

[6] 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).

that if there are 10 non-U.S. citizen respondents, based on other information collection STA burdens, they will spend approximately 0.25 hours to compile and submit the information, a total of 2.5 burden hours. Should TSA require a fingerprint based criminal history records check, there would be an additional time burden of approximately 2 hours per respondent, a total of 20 burden hours.

For this collection, TSA estimates the total annual respondents to be 846 and the total annual hour burden to be 210,684 hours.

Dated: April 13, 2026.

Christina A. Walsh,

Paperwork Reduction Act Officer,

Information Technology,

Transportation Security Administration.

[FR Doc. 2026-07364 Filed: 4/15/2026 8:45 am; Publication Date: 4/16/2026]