[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request an Extension 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 an extension in compliance with the Paperwork Reduction Act (PRA). On October 26, 2022, OMB approved TSA's request for an emergency approval of this collection to address the ongoing cybersecurity threat to surface transportation and associated infrastructure. TSA is now seeking to renew the collection, which expires on April 30, 2023, with incorporation of the subject of the emergency request. The ICR describes the nature of the information collection and its expected burden. The collection allows TSA to address the ongoing cybersecurity threat to surface transportation systems and associated infrastructure.

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 (IT), 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 http://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 U.S.C. § 114(*l*)(2),[5] TSA has the authority to issue Security Directives (SDs) if the

---

[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).
[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 security directive must be issued

Administrator of TSA determines that a regulation or SD must be issued immediately in order to protect transportation security.

On November 30, 2021, OMB approved TSA's request for an emergency approval of this information collection to address the ongoing cybersecurity threat to surface transportation and associated infrastructure. On April 7, 2022, TSA submitted an extension request to OMB, which was approved on October 25, 2022. *See* ICR Reference Number 202203-1652-003. On October 26, 2022, OMB approved TSA's request for an additional emergency approval, revising this information collection. *See* ICR Reference Number: 202210-1652-001. The collection covers both mandatory reporting and voluntary reporting of information. The OMB approval allowed for the additional institution of mandatory reporting requirements and collection of information voluntarily submitted. *See* ICR Reference Number: 202111-1652-003. TSA is now seeking renewal of this information collection for the maximum three-year approval period.

The request for a revised collection was necessary as a result of actions TSA took to address the ongoing cybersecurity threats to the United States' national and economic security posed by this threat to surface transportation and associated infrastructure. On October 18, 2022, TSA issued SD 1580/1582-2022-01 *Rail Cybersecurity Mitigation Actions, Contingency Planning, and Testing,* which applies to Owner/Operators including the "Higher Risk" freight railroads identified in 49 CFR 1580.101 and additional TSA-designated freight and passenger railroads. This SD became effective on October 24, 2022. The emergency request did not affect the previously-approved collection for SD 1580-21-01 and SD 1582-21-01, which remain in effect, mandating TSA-specified Owner/Operators of "higher risk" railroads and rail transit systems, respectively, to

---

immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.

implement an array of cybersecurity measures to prevent disruption and degradation to their infrastructure.[6] The scope of these SDs align with the railroads and rail transit systems required to report significant security incidents to TSA under 49 CFR 1570.203.

In addition, the emergency request did not affect the previously-issued "information circular" (IC), which remain in effect. The IC contains non-binding recommendations with the same measures for railroad Owner/Operators, public transportation agencies, rail transit system Owner/Operators, and certain over-the-road bus Owner/Operators not specifically covered under SDs 1580-21-01 or 1582-21-01.

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 plans to collect the following information:

A. SD 1580/82-2022-01 includes the following requirements:

1. The Cybersecurity Implementation Plan submitted to TSA for approval that addresses how the Owner/Operator will achieve each of the following prescribed objectives in the SD:
    - identification of the Owner/Operator's Critical Cyber Systems;
    - implementation of network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised;

[6] Companies and agencies that are identified as higher-risk service the regions with the highest surface transportation-specific risk. Risk ranking is based on considerations related to ridership, location of services provided (use of the same stations and stops), and relationship between feeder and primary systems. *See* https://www.tsa.gov/sites/default/files/guidance-docs/high_threat_urban_area_htua_group_designations_0.pdf

- implementation of access control measures to secure and prevent unauthorized access to critical cyber systems;
- implementation of continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and;
- reduction of the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on Critical Cyber Systems in a timely manner using a risk-based methodology.

2. The Annual Audit Plan for the Cybersecurity Assessment Program 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.
3. Provide documentation as necessary to establish compliance, to be provided upon TSA request.

B. ***SD 1580-21-01, SD 1582-21-01, and IC 2021-01*** remain in effect and include the following information collection requirements for the SDs and recommendations for the IC:

1. Designate a Cybersecurity Coordinator who is available to TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise.
2. Report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA).
3. Develop a cybersecurity incident response plan.
4. Complete a cybersecurity vulnerability assessment to address cybersecurity gaps using the form provided by TSA.

TSA, in conjunction with federal partners such as CISA, will use 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 will also use the information to inform timely modifications to cybersecurity requirements to improve transportation security and national economic security. TSA will use the collection of information to ensure compliance with TSA's cybersecurity measures required by the SDs and the recommendations under the IC.

Certification of completion of SD requirements

The SDs and IC took effect on October 24, 2022. Within 7 days of the effective date of the SDs, Owner/Operators must provide their designated Cybersecurity Coordinator information; within 90 days of the effective date of the SDs, Owner/Operators must submit their Cybersecurity Implementation Plan; within 120 days of the effective date of the SDs, Owner/Operators must complete the Vulnerability Assessment (TSA form); within 180 days of the effective date of the SDs, Owner/Operators must adopt a Cybersecurity Incident Response Plan; and within 7 days of completing the Cybersecurity Incident Response Plan requirement, Owner/Operators must submit a statement to TSA via email certifying that the Owner/Operator has completed this requirement. Owner/Operators can complete and submit the required information via email or other electronic options provided by TSA. Documentation of compliance must be provided upon request. As the measures in the IC are voluntary, the IC does not require Owner/Operators to report on their compliance.

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.[7]

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 IC 2021-01 apply to 457 railroad Owner/Operators, 115 public transportation agencies and rail transit system Owner/Operators, and 209 over-the-road bus Owner/Operators, for a total of 781 respondents. For this collection, TSA estimates the total annual respondents to be 854 and the total annual hour burden to be 134,023 hours.

Dated: November 7, 2022.

Christina A. Walsh,

TSA Paperwork Reduction Act Officer,

Information Technology.

[FR Doc. 2022-24621 Filed: 11/10/2022 8:45 am; Publication Date: 11/14/2022]

[7] In addition, all data in TSA systems are statutorily required to comply with the Federal Information Security Modernization Act 2014 (FISMA) 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 FISMA 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).