[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request a Revision from OMB of One Current Public Collection of Information: Pipeline Corporate Security Reviews and TSA Security Directive Pipeline-2021-02 series

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 1652–0056, abstracted below, that we will submit to OMB for an extension in compliance with the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. The collection allows TSA to assess the current security practices in the pipeline industry through TSA's Pipeline Corporate Security Review (CSR) program and allows for the continuation of mandatory cybersecurity requirements under the TSA Security Directive (SD) Pipeline-2021-02 series.

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 1652-0056; Pipeline Corporate Security Reviews and TSA Security Directive Pipeline-2021-02 series. Under the Aviation and Transportation Security Act[1] and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for "security in all modes of transportation . . . including security responsibilities . . . over modes of transportation that are exercised by the Department of Transportation."[2] TSA is specifically empowered to assess threats to

[1] Pub. L. 107-71 (115 Stat. 597, Nov. 19, 2001), codified at 49 U.S.C. 114.

[2] *See* 49 U.S.C. 114(d). The TSA Administrator's current authorities under the Aviation and Transportation Security Act have been delegated to him by the Secretary of Homeland Security. Section 403(2) of the Homeland Security Act of 2002, Pub. L. 107-296 (116 Stat. 2135, Nov. 25, 2002), transferred all functions of TSA, including those of the Secretary of Transportation and the Under Secretary of

transportation;[3] develop policies, strategies, and plans for dealing with threats to transportation;[4] oversee the implementation and adequacy of security measures at transportation facilities;[5] and carry out other appropriate duties relating to transportation security.[6] The Implementing Recommendations of the 9/11 Commission Act of 2007 included a specific requirement for TSA to conduct assessments of critical pipeline facilities.[7]

Pursuant to its authority, TSA may, at the discretion of the Administrator, assist another Federal agency, such as the Cybersecurity and Infrastructure Security Agency, in carrying out its authority in order to address a threat to transportation.[8] As noted above, TSA issued the SD Pipeline-2021-02 series in order to protect transportation security and critical infrastructure. *See* 49 U.S.C. 114(*l*)(2).

Consistent with these authorities and requirements, TSA developed the voluntary Pipeline CSR program and the mandatory SD Pipeline 2021-02 series to assess the current security practices in the pipeline industry, with a focus on the physical and cyber security of pipelines and the crude oil and petroleum products, such as gasoline, diesel, jet fuel, home heating oil, and natural gas, moving through the system infrastructure.

TSA is revising the title of the collection from "Pipeline Corporate Security Reviews and Security Directives" to "Pipeline Corporate Security Reviews and TSA Security Directive Pipeline-2021-02 series." This title more accurately reflects the specific TSA SD associated with this collection. TSA is seeking renewal of this information collection for the maximum 3-year approval period.

Transportation of Security related to TSA, to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.2, the Secretary delegated to the Administrator of TSA, subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including that in section 403(2) of the Homeland Security Act.

[3] 49 U.S.C. 114(f)(2).

[4] 49 U.S.C. 114(f)(3).

[5] 49 U.S.C. 114(f)(11).

[6] 49 U.S.C. 114(f)(15).

[7] *See* section 1557 of Pub. L. 110-53 (121 Stat. 266, Aug. 3, 2007) as codified at 6 U.S.C. 1207.

[8] *Id.* § 114(m), granting the TSA Administrator the same authority as the FAA Administrator under 49 U.S.C. 106(m).

Establishing Compliance with Voluntary Pipeline CSR Program Information Collection Requirements

Pipeline CSRs are voluntary, face-to-face visits, usually at the headquarters facility of the pipeline Owner/Operator. TSA has developed a Question Set to aid in the conducting of CSRs. The CSR Question Set structures the TSA and pipeline Owner/Operator discussion and is the central data source for the physical security information TSA collects. TSA developed the CSR Question Set based on input from government and industry stakeholders on how best to obtain relevant information from a pipeline Owner/Operator about its security plan and processes.

This CSR information collection provides TSA with real-time information on a company's physical security posture. The relationships these face-to-face contacts foster are critical to the Federal government's ability to reach out to the pipeline stakeholders affected by the CSRs. In addition, TSA follows up via email with Owner/Operators on specific recommendations made by TSA during the CSR.

Establishing Compliance with Mandatory TSA SD Pipeline-2021-02 series Information Collection Requirements

While the CSR collection supports physical security plans and processes, TSA issued the SD Pipeline-2021-02 series with mandatory requirements in order to mitigate specific cyber security concerns posed by current threats to national security.

The mandatory TSA SD series information collection requirements are as follows:

a. Pipeline Owner/Operators designated by TSA as critical must submit a Cybersecurity Implementation Plan (CIP) to TSA for approval (there is no designated form or format). Once approved by TSA, pipeline Owner/Operators must implement and maintain all measures. Owner/Operators must submit changes to their CIP for approval in accordance with the guidance in the SD. CIPs must be made available to TSA upon request.

b. Pipeline Owner/Operators designated by TSA as critical must develop and maintain an up-to-date Cybersecurity Incident Response Plan (CIRP) for their designated critical cyber systems to reduce the risk of operational disruption, or the risk of other significant impacts on business critical functions. Owner/operators must test the effectiveness of the CIRP no less than annually. There is no designated form or format for the CIRP. Owner/Operators must submit the CIRP to TSA upon request.

c. Pipeline Owner/Operators designated by TSA as critical must submit a Cybersecurity Assessment Plan (CAP) on an annual basis to TSA for approval (there is no designated form or format). The plan must include a schedule for auditing and assessing at least one-third of the policies, procedures, measures and capabilities in the CIP each year. Owner/Operators must also submit a CAP annual report to TSA of the results of assessments conducted in accordance with the approved plan.

d. Pipeline Owner/Operators designated by TSA as critical must make records to establish compliance with the SD Pipeline-2021-02 series available to TSA upon request for inspection and/or copying.

Submissions by pipeline Owner/Operators in compliance with the voluntary Pipeline CSR or the mandatory SD Pipeline-2021-02 series requirements are deemed Sensitive Security Information and are protected in accordance with procedures meeting the transmission, handling, and storage requirements of Sensitive Security Information set forth in part 1520 of title 49, Code of Federal Regulations.

Annual Burden Discussion

For the voluntary Pipeline CSR program, TSA estimates that they will conduct 21 security reviews per year, each involving a pipeline security manager. TSA estimates that each CSR will last a total of 8 hours, and then include a follow-up regarding security recommendations, lasting up to 3 hours. The total time burden for this task is 231 hours

((1 security manager x 8 hours x 21 entities = 168 hours) + (1 individual x 3 hours x 21 entities = 63 hours)).

For the mandatory information collections required by the SD Pipeline-2021-02 series, all designated pipeline Owner/Operators have submitted and approved CIPs. TSA estimates that a total of 100 Owner/Operators will continue to update their CIPs and submit changes to TSA for approval as necessary as cyber controls are updated or changed. The burden is therefore the estimated time annually to keep the CIP current and provide changes to TSA for approval as necessary. TSA estimates updates to the CIP will be conducted by a team consisting of a cybersecurity manager and four cybersecurity analysts/specialists. TSA assumes the team will spend 2 weeks updating the implementation plan; therefore, the time burden for this task is 40,000 hours (5 individuals x 40 hours x 2 weeks x 100 entities).

All designated pipeline Owner/Operators have established CIRPs. TSA estimates 100 entities will update their CIRPs annually. TSA assumes one cybersecurity manager will spend 2 weeks updating the CIRP; therefore, the time burden for this task is 8,000 hours (1 individual x 40 hours x 2 weeks x 100 entities).[9]

All designated pipeline Owner/Operators have a TSA approved CAP. TSA estimates 100 entities will submit an annual plan for their CAP and an annual report. TSA estimates that two people, a cybersecurity manager and an audit compliance manager will spend an average of 2 weeks developing and submitting the plan and report; therefore, the time burden for this task is 16,000 hours (2 individuals x 40 hours x 2 weeks x 100 entities).

TSA estimates 100 entities will work to ensure compliance documentation is kept up to date. TSA estimates that two people, a cybersecurity manager and an audit

[9] There is no requirement for Owner/Operators to submit CIRPs unless requested by TSA. In February 2022, under the provisions of the SD Pipeline 2021-02 series and at TSA's request, pipeline Owner/Operators provided their CIRPs to TSA.

compliance manager will spend an average of 2 weeks updating compliance documentation; therefore, the time burden for this task is 16,000 hours (2 individuals x 40 hours x 2 weeks x 100 entities).

TSA estimates the total annual burden hours for the mandatory collection to be 80,231 hours (Pipeline CSR- 231, CIP – 40,000, CIRP-8,000, CAP and annual report - 16,000, Compliance Documentation-16,000).

Dated: July 29, 2025.

Christina A. Walsh,

Paperwork Reduction Act Officer,

Information Technology

Transportation Security Administration.

[FR Doc. 2025-14538 Filed: 7/31/2025 8:45 am; Publication Date: 8/1/2025]