**[9110-05-P]**

**DEPARTMENT OF HOMELAND SECURITY**

**Transportation Security Administration**

**Intent to Request an Extension from OMB of One Current Public Collection of Information: Pipeline Corporate Security Review Program**

**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). On July 29, 2022, OMB approved TSA's request for an emergency revision of this collection to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. TSA is now seeking to renew the collection, which expires on January 31, 2023, with incorporation of the subject of the emergency revision. 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 (PCSR) program and allows for the continued institution of mandatory cybersecurity requirements under the TSA Security Directive (SD) Pipeline 2021-02 series. The PCSR program is part of the larger domain awareness, prevention, and protection program supporting TSA's and the Department of Homeland Security's missions. The updated ICR reflects changes to collection requirements based on TSA's update to the TSA SD 2021-02 series, released on July 21, 2022.

**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 1652-0056; Pipeline Corporate Security Review (PCSR) Program*. Under the Aviation and Transportation Security Act[1] and delegated authority from the Secretary of Homeland Security, TSA has broad responsibility and authority for

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

"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 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 (9/11 Act) 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 PCSR program 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. In addition, TSA issued SD 2021-02 in July 2021 and revised the information collection requirements based on the mandatory requirements in SD 2021-

---

[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 (HSA) 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 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 HSA.
[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).

02. This ICR was approved by OMB on July 15, 2021. *See* ICR Reference Number: 202107-1652-002.

*Establishing Compliance with Voluntary Pipeline Corporate Security Review (PCSR) Program Information Collection Requirements*

PCSRs 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 PCSRs. The PCSR Question Set structures the TSA-Owner/Operator discussion and is the central data source for the security information TSA collects. TSA developed the PCSR 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 PCSR information collection provides TSA with real-time information on a company's 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 PCSRs. In addition, TSA follows up via email with Owner/Operators on specific recommendations made by TSA during the PCSR.

While the PCSR collection supports security plans and processes, TSA has issued the SDs with mandatory requirements in order to mitigate specific security concerns posed by current threats to national security.

*Establishing Compliance with Mandatory TSA Security Directive 2021-02 Information Collection Requirements (Emergency Revision)*

On July 15, 2021, OMB approved TSA's requests for an emergency revision of this information collection, allowing for the institution of mandatory requirements issued within TSA's SD 2021-02, on July 19, 2021. *See* ICR Reference Number: 202107-1652-002. SD 2021-02 mandated regulated entities to (1) implement critically important mitigation measures to reduce the risk of compromise from a cyberattack; (2) develop

and maintain an up-to-date Cybersecurity Contingency/Response Plan; and (3) test the effectiveness of the operator's cybersecurity practices through an annual cybersecurity architecture design review. In the renewal process of the ICR, TSA published two *Federal Register* notices on August 27, 2021 and November 15, 2021, respectively, requesting public comment on the information collection requirements for SD 2021-02. Subsequently, on July 26, 2022, OMB approved TSA's request to extend the information collection. *See* ICR Reference Number: 202111-1652-001.

On July 21, 2022, TSA issued SD 2021-02C, amending the SD 2021-02 series. This revision was necessary to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. SD 2021-02C provides Owner/Operators with more flexibility to meet the intended security outcomes while ensuring sustainment of the cybersecurity enhancements accomplished through this SD series.

Overall, SD 2021-02C changed the cybersecurity requirements from a prescriptive approach to a security outcome approach. SD 2021-02C also changed the scope of requirements to Critical Cyber Systems, as defined in the SD, and changed cybersecurity assessment requirements. There was no change to the applicability of the SD to Owner/Operators of hazardous liquid and natural gas pipelines or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical.

On July 29, 2022, OMB approved TSA's request for the emergency revision of this information collection, allowing for the institution of mandatory requirements issued within TSA SD 2021-02C. *See* ICR Reference Number: 202207-1652-001.

SD 2021-02C requires identified Owner/Operators to meet three requirements:

1. Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures employed and the schedule for achieving the outcomes described in the SD; and provide to TSA upon request.

2. Develop and maintain a record of an up-to-date Cybersecurity Incident Response Plan to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity, as defined in this SD, should the Information and/or Operational Technology systems of a gas or liquid pipeline be affected by a cybersecurity incident; and provide to TSA upon request.

3. Establish a Cybersecurity Assessment Program and submit an annual 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; and provide to TSA upon request.

*The following is a summary of the information collection requirements:*

1. Voluntary PCSR information collection requirements: Owner/Operators complete PCSR Question Set and follow-up requests.

2. Mandatory TSA SD information collection requirements:

a. Owner/Operators must submit a Cybersecurity Implementation Plan to TSA for approval, no later than October 25, 2022 (90 days after the effective date of the SD). Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan within the schedule as stipulated in the plan.

b. Consistent with the previous requirement in the SD 2021-02 series, Owner/Operators must have an up-to-date Cybersecurity Incident Response Plan. Owner/Operators must submit this Plan to TSA, upon request.

c. The Owner/Operator must submit an annual plan for their Cybersecurity Assessment Program to TSA, no later than 60 days after TSA's approval of the Owner/Operator's Cybersecurity Implementation Plan. The plan must describe the Cybersecurity Assessment Program required by the SD, including the schedule for specific actions.

d. Owner/Operators must make records to establish compliance with SD 2021-02C available to TSA upon request for inspection and/or copying.

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

*Annual Burden Discussion*

For the voluntary PCSR program, the annual hour burden is estimated to be 220 hours based upon 20 PCSR visits per year, each lasting a total of eight hours, and the follow-up regarding security recommendations, lasting up to three hours ((20 x 8 = 160 hours) + (20 x 3 = 60 hours) = 220 hours).

For the mandatory information collections required by SD 2021-02C, TSA estimates a total of 100 Owner/Operators will provide TSA with their Cybersecurity Implementation Plan, their annual plan for their Cybersecurity Assessment Program and, upon request, documentation to establish compliance to include their Cybersecurity Incident Response Plans.

TSA estimates 100 entities will develop a Cybersecurity Implementation Plan, and the plan will be developed by a team consisting of a cybersecurity manager and four cybersecurity analysts/specialists. TSA assumes the team will spend two weeks developing the implementation plan; therefore, the time burden for this task will be 40,000 hours (5 individuals x 40 hours x 2 weeks.)

TSA estimates 100 entities will establish and update their Cybersecurity Incident Response Plans annually, and the time burden to produce this update is 80 hours (total – 8,000 hours).[9]

TSA estimates 100 entities will submit an annual plan for their Cybersecurity Assessment Program, and the time burden for submitting an annual audit plan to TSA is 40 hours (total – 4,000 hours).

TSA estimates 100 entities will develop compliance documentation and the time burden for this requirement is 80 hours (total 8,000 hours).

TSA estimates the total annual burden hours for the mandatory collection to be 20,220 hours (PCSR-220, Cybersecurity Incident Response Plan-8,000, Annual Plan for Cybersecurity Assessment-4,000, Compliance Documentation-8,000). In addition, the one-time burden for the development and submission to TSA of the Owner/Operator's Cybersecurity Implementation Plan is 40,000 hours.

TSA is seeking renewal of this information collection for the maximum three-year approval period.

Dated: September 28, 2022.

Christina A. Walsh,

*TSA Paperwork Reduction Act Officer,*

*Information Technology.*

[FR Doc. 2022-21400 Filed: 9/30/2022 8:45 am; Publication Date: 10/3/2022]

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