INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Corporate Security Review (PCSR)
OMB control number 1652-0056
Exp.: 01/31/2022

1. Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information. (Annotate the CFR parts/sections affected).

The Transportation Security Administration (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." 49 U.S.C. 114(d). In addition to carrying out the security responsibilities in paragraph (d), TSA is responsible for "assess[ing] threats to transportation" and "develop[ing] policies, strategies, and plans for dealing with threats to transportation security." 49 U.S.C. 1114(f)(2) and (3). Congress has recognized TSA's responsibility for pipeline security by requiring TSA to conduct assessments of pipeline security systems. *See* section 1557 of the Implementing Recommendations of the 9/11 Commission Act (Pub. L. 110-53; 121 Stat. 475; Aug. 3, 2007), as codified at 6 U.S.C. 1207.

In order to assess current industry security practices, TSA implemented its Pipeline Corporate Security Review (PCSR) program. The PCSR is a voluntary, face-to-face visit with a pipeline owner/operator during which TSA discusses the company's corporate level security planning and also completes the PCSR Form, which includes 210 questions concerning the owner/operator's corporate level security planning, covering security topics such as physical and cyber security, vulnerability assessments, training, and emergency communications. TSA also follows up on results of each PCSR.

On July 15, 2021, OMB approved TSA's request for an emergency revision of this information collection, allowing for the institution of mandatory cybersecurity requirements. *See* ICR Reference Number: 202107-1652-002. The revision was necessary as a result of actions TSA took to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. Specifically, on July 19, 2021, TSA issued a Security Directive (SD) applicable to owner/operators of critical hazardous liquid and natural pipelines and liquefied natural gas facilities.[1] To protect against the ongoing cybersecurity threat, TSA relied on its authority to impose requirements on these owner/operators of TSA-specified owner/operators of gas and liquid pipelines, including implementing an array of cybersecurity measures, to prevent disruption and degradation to this critical transportation infrastructure. This SD was issued in coordination with the Cybersecurity and Infrastructure

[1] On May 28, 2021, TSA issued another SD which included three information collections. OMB control number 1652-0055, includes two of these information collections, requiring owner/operators to report cybersecurity incidents to CISA, and to designate a Cybersecurity Coordinator, who is required to be available to the TSA 24/7 to coordinate cybersecurity practices and address any incidents that arise, and who must submit contact information to TSA. OMB control number 1652-0050 contains the remaining information collection, requiring owner/operators to conduct a cybersecurity assessment, to address cyber risk, and identify remediation measures that will be taken to fill those gaps and a time frame for achieving those measures.

Security Agency (CISA). Under 49 U.S.C. 114(l)(2),[2] TSA has authority to immediately issue security directives if the Administrator of TSA determines that actions are needed to protect transportation security. TSA also has authority, at the discretion of the Administrator, to assist another Federal agency in carrying out its authority in order to address a threat to transportation. *See* 49 U.S.C. 114(m).[3]

TSA is seeking an extension of this collection beyond the six-month approval granted under the emergency request.

2. Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection.

Voluntary Collection. As required by 6 U.S.C. 1207, TSA has used the information collected during the PCSR process to determine baseline security standards and areas of security weakness in the pipeline mode. This data and interaction with stakeholders informs the agency's Pipeline Security Guidelines and Pipeline Security Best Practice Observation documents.

Mandatory Collection: OMB approved TSA's emergency request to revise the collection to require owner/operators to implement the following collections of information:

1. Cybersecurity Contingency/Response Plan

   Owner/Operators are required to develop and adopt a Cybersecurity Contingency/Response Plan to ensure the resiliency of their operations in the event of a cybersecurity attack. Owner/operators must provide evidence of compliance to TSA upon request.

2. Third-Party Evaluation

   Owner/Operators are required to have a third-party complete an evaluation of their industrial control system design and architecture to identify previously unrecognized vulnerabilities. This evaluation must include a written report detailing the results of the evaluation and the acceptance or rejection of any recommendations provided by the evaluator to address vulnerabilities. This written report must be made available to TSA upon request and retained for no less than 2 years from the date of completion.

3. Certification of completion of SD requirements

   Within 7 days of the deadlines set forth in the SD, owner/operators must ensure that their Cybersecurity Coordinator or other accountable executive submits a statement to TSA via email certifying that the owner/operator has met the requirements of the SD. Owner/Operators can complete and submit via email an optional TSA form for each

[2] 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 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.

[3] 49 U.S.C. 114(m) grants the TSA Administrator the same authority as the Administrator of the Federal Aviation Administration under 49 U.S.C. 106(m), and is applicable to all modes of transportation.

submission deadline. TSA requires the certifications be made in a timely way. Documentation of compliance must be provided upon request.

3. Describe whether, and to what extent, the collection of information involves the use of automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submission of responses, and the basis for the decision for adopting this means of collection. Also describe any consideration of using information technology to reduce burden.

The voluntary collection is conducted by means of a site visit to a pipeline owner/operator's headquarters location. During the site visit, TSA discusses the owner/operator's security planning, and all information captured during the visit is later recorded electronically by TSA onto the PCSR Workbook. This collection workbook is secured and retained electronically by TSA upon completion and used for analysis in determining industry baseline standards. The intent of the PCSR program is to verify that the owner/operator is implementing its security program through an onsite review of its security plan as well as to provide a means for TSA to build stakeholder relations through a face-to-face discussion on security planning, a goal which is not readily achievable or practicable if an electronic reporting option were available to the owner/operator as an alternative to the onsite visit.

Regarding the mandatory collection, TSA requires collection of information and maintenance of records to establish compliance with its security directives. For example, TSA requires owner/operators to submit a statement that they have complied with requirements within the established deadline. Such statements can be made by e-mail. For convenience, TSA provides an optional form for each submission deadline that owner/operators can complete and submit via email. To the extent the information submitted is Sensitive Security Information (SSI), TSA will handle as required by 49 CFR parts 15 and 1520.

4. Describe efforts to identify duplication. Show specifically why any similar information already available cannot be used or modified for use for the purpose(s) described in Item 2 above.

TSA works closely with its partners at the U.S. Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) to coordinate security initiatives. Since 2006, the two agencies have operated under an annex to the memorandum of understanding (MOU) between DOT and the Department of Homeland Security. This annex specifically addresses the respective roles and responsibilities of TSA and PHMSA as well as coordination processes. There is no other similar information collection currently in place at PHMSA that specifically targets corporate-level security planning and plan implementation in the pipeline mode of transportation.

Regarding the mandatory submission, TSA developed the requirements in consultation with CISA and in coordination with PHMSA as well as the Department of Energy and other applicable agencies. TSA has determined that no other agency requires submission of the type of information TSA may collect related to its security directives. These include no other cybersecurity measures, Cybersecurity Contingency/Response Plan or Third Party Evaluation and described certifications so no similar information is available to be used by DHS.

5. If the collection of information has a significant impact on a substantial number of small businesses or other small entities (Item 5 of the Paperwork Reduction Act submission form), describe the methods used to minimize burden.

This information collection should not have a significant impact on small businesses or other small entities. While there are over 2,200 pipeline owner/operators in the United States, the PCSR primarily focuses on the nation's top 100 pipeline operators, primarily determined by energy throughput. These top 100 operators account for 85 percent of all hazardous liquids and natural gas transported in the United States. These companies are often large, corporate operations with business ventures across the world, and as such, employ hundreds if not thousands of employees. By focusing the PCSR on the top 100 pipeline operators in the United States, TSA is aligning its mission and resources with DHS's risk-based security approach. It is possible that TSA will visit pipeline operators outside the top 100, but only as circumstances dictate (*e.g.*, intelligence information indicates a smaller system is the target of a credible threat, or smaller systems are of critical importance to national defense). Given that the PCSR program only visits approximately 20 out of 2,200 owner/operators a year, and the owner/operators visited often represent the largest pipeline companies in the United States, there should be no significant impact on a substantial number of small pipeline owner/operators in any given year of the program.

Regarding the mandatory submission, the SD applies to TSA identified critical pipeline owner/operators. The collection of information required by the SD does not have a significant impact on a substantial number of small businesses as the vast majority of these companies are large, corporate operations with business ventures across the world, and as such, employ hundreds if not thousands of employees.

6. Describe the consequence to Federal program or policy activities if the collection is not conducted or is conducted less frequently, as well as any technical or legal obstacles to reducing burden.

If the PCSR collection were to be discontinued, this would seriously impede TSA's ability to remain current on minimum security standards being voluntarily employed in the industry, as well as diminish its ability to identify areas of security weakness, two activities that are critical to the agency in carrying out its transportation security mission. Without means of collecting this information, TSA would be unable to confidently identify security gaps and weakness in the pipeline mode and, consequently, would not be able to effectively identify areas to develop programs to better strengthen modal security.

Without the mandatory collection, TSA will be unable to address the critical threat to the nation's pipeline systems, which is reasonably likely to result in public harm. For example, if an attack occurred against a pipeline and TSA did not have this collection, pipeline owner/operators may not have cybersecurity response plans in place and third party assessment of their cybersecurity architecture. These measures decrease the impact of a cybersecurity incident affecting critical infrastructure and increase an operator's awareness of possible vulnerabilities.

7. Explain any special circumstances that require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

There are no special circumstances that would require the collection to be conducted in a manner inconsistent with the general information collection guidelines in 5 CFR 1320.5(d)(2).

8. Describe efforts to consult persons outside the agency to obtain their views on the availability of data, frequency of collection, the clarity of instructions and recordkeeping, disclosure, or reporting format (if any), and on the data elements to be recorded, disclosed, or reported. If applicable, provide a copy and identify the date and page number of publication in the Federal Register of the agency's notice, required by 5 CFR 1320.8(d) soliciting comments on the information collection prior to submission to OMB. Summarize public comments received in response to that notice and describe actions taken by the agency in response to these comments. Specifically address comments received on cost and hour burden.

TSA invited public comment on this information collection requirement, a 60-day notice was published in the *Federal Register* on August 27, 2021 (86 FR 48239) and a 30-day notice was published on November 15, 2021 (86 FR 63050). TSA received no comments. Since July, 2021, TSA has answered over 245 questions from pipeline operators about the SD and participated in three industry-led meetings to discuss the SD requirements.

9. Explain any decision to provide any payment or gift to respondents, other than remuneration of contractors or grantees.

No payment or gift will be provided to respondents.

10. Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy.

No assurances of confidentiality were provided to respondents; however, to the extent permissible under the law, DHS will seek to protect the trade secrets and commercial and financial information of the pipeline owner/operators. Also, to the extent information collected is deemed SSI, TSA will handle as required by 49 CFR parts 15 and 1520. In addition, Privacy Impact Assessment (PIA) coverage is provided under the DHS/ALL/PIA-006 General Contact Lists PIA. (June 15, 2007).

11. Provide additional justification for any questions of sensitive nature, such as sexual behavior and attitudes, religious beliefs, and other matters that are commonly considered private.

No personal questions of a sensitive nature will be posed during the information collection.

12. Provide estimates of hour and cost burden of the collection of information.

In regards to the voluntary collection, TSA anticipates completing 20 PCSRs annually. Each PCSR places an 8-hour burden on a respondent, and an additional 3 hours to follow-up on results of each PCSR, for an annual hour burden of 11 hours. The annual hour burden for the

entire collection is 220 hours. TSA uses a fully-loaded wage rate[4] of $92.67 for a Corporate Security Manager.[5] TSA estimates an annual hour burden cost to the public of $20,387. Table 1 summarizes these results.

Table 1: Annual Costs for Pipeline Corporate Security Reviews

Activity	Number of Annual Responses A	Hour Burden per Response B	Annual Hour Burden C = A x B	Annual Hour Burden Cost D = C x $92.67
PCSR	20	8	160	$14,827
PCSR Re-interview	20	3	60	$5,560
Total	40	11	220	$20,387

Regarding the mandatory collection, TSA estimates that 97 entities will develop cybersecurity contingency response plans, conduct evaluations of the cybersecurity response plans by 3rd parties, and certify the results of the 3rd party cybersecurity evaluations. TSA estimates that it takes 80 hours to develop each contingency response plan, 42 hours to conduct a 3rd party evaluation, and 8 hours to complete the Certification of completion of SD requirements, for a total of 130 hours per respondent. The time burden to the public will be 97 respondents × 130 hours = 12,610 hours. TSA assumes these tasks will be done by a corporate cybersecurity coordinator, with a fully-loaded wage rate of $106.17.[6] These are one-time burdens that will occur during the first year of this collection, and the total cost burden for these one-time tasks is $1,338,766 = 12,610 × $106.17.

TSA estimates the total respondents for the information collection is 97 and the combined annual burden hours for the voluntary and mandatory collections are 13,270 hours = 12,610 (one-time burden) + 220 (Year 1 annual burden) + 220 (Year 2 annual burden) + 220 (Year 3 annual burden) = 13,270 hours, or an annual average of 4,423.33 hours.

The total cost for this collection to the public is $1,338,766 + $20,387 = $1,359,152 in Year 1, $20,387 in Year 2, and $20,387 in Year 3, or $1,399,926 over the 3-year period of collection.

---

[4] A fully-loaded wage rate accounts for non-salary cost of employee compensation, such as health and retirement benefits.

[5] The unloaded wage rate for a General and Operations Manager is $61.30. BLS. May 2020 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. SOC 11-1021 General and Operations Managers. Last modified March 31, 2021 (accessed June 23, 2021). https://www.bls.gov/oes/2020/May/naics3_486000.htm. To load the wage rate, TSA calculates a load factor to inflate the wage rate to account for benefits. The load factor is 1.511704. BLS. Employer Costs for Employee Compensation - December 2020. Table 5. Employer costs per hour worked for employee compensation and costs as a percent of total compensation: private industry workers. Production, transportation and material moving occupations. Last modified March 18, 2021 (accessed June 23, 2021). https://www.bls.gov/news.release/archives/ecec_03182021.htm. The fully-loaded wage rate is $61.30 × 1.511704 = $92.67.

[6] The unloaded wage rate for a Cybersecurity Coordinator is $70.23. BLS. May 2020 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. SOC 11-3021 Computer and Information Systems Managers. Last modified March 31, 2021 (accessed September 29, 2021). https://www.bls.gov/oes/2020/May/naics3_486000.htm. The fully-loaded wage rate is $70.23 × 1.511704 = $106.17.

13. Provide an estimate of annualized capital and start-up costs. (Do not include the cost of any hour burden shown in Items 12 and 14).

TSA does not estimate a cost to the pipeline industry beyond the hour burden detailed in answer 12.

14. Provide estimates of annualized cost to the Federal Government. Also, provide a description of the method used to estimate cost, and other expenses that would not have been incurred without this collection of information.

A PCSR is conducted by one (1) representative from TSA; either a Senior Analyst (J Band) or a Junior Analyst (I Band). Each review takes approximately 8 hours per employee. Following the review, an additional 32 hours are devoted to completing the form, which is split equally between two analysts, for an annual hour burden of 800 hours. TSA I-Band employees have an average fully-loaded wage rate of $72.73. TSA J-Band employees have an average fully-loaded wage rate of $85.80. TSA uses a simple average wage rate of $79.26 to estimate the hour burden costs, for an annual hour burden cost of $63,410. Table 2 summarizes these estimates.

Table 2: TSA PCSR Hour Burden and Costs

Activity	Number of Annual Responses A	Hour Burden per Response B	Annual Hour Burden C = A x B	Annual Hour Burden Cost D = C x $79.26
PCSR	20	8	160	$12,682
PCSR Follow-up	20	32	640	$50,728
Total	**40**		**800**	**$63,410**

TSA also budgets an estimated $41,000 in travel costs to support the PCSR process. This brings the total TSA annual costs $114,410, or $313,230 over three years.

In addition, TSA has one-time costs to ensure compliance with the Security Directive (SD). TSA estimates 2 compliance inspectors will expend 24 hours (3 work days) per pipeline company (97) for this task. Using the $79.26 wage rate shown above, the one-time cost to TSA to ensure SD compliance is estimated to be $369,047 (2 inspectors x 24 hours x $79.26 x 97 companies). The total cost of this information collection to TSA over a three-year period is estimated to be $313,230 (annual costs) + $369,047 (one-time costs) = $682,277.

15. Explain the reasons for any program changes or adjustments reported in Items 13 or 14 of the OMB Form 83-I.

There are no program changes or adjustments, except TSA is now including the burden estimates for the mandatory part of the collection.

16. For collections of information whose results will be published, outline plans for tabulation and publication. Address any complex analytical techniques that will be used. Provide the time schedule for the entire project, including beginning and ending dates of the collection of information, completion of report, publication dates, and other actions.

Security information collected during the PCSR will not be published or shared. To the extent information collected via the PCSR process is considered to be SSI, it will be protected from disclosure and publication, and will be handled as described in 49 CFR parts 15 and 1520.

Regarding the mandatory collection, no information resulting from the collections under the SD will be published.

17. If seeking approval to not display the expiration date for OMB approval of the information collection, explain the reasons that display would be inappropriate.

Not applicable.

18. Explain each exception to the certification statement identified in Item 19, "Certification for Paperwork Reduction Act Submissions," of OMB Form 83-I.

No exceptions noted.