INFORMATION COLLECTION SUPPORTING STATEMENT

Critical Facility Information of the Top 100 Most Critical Pipelines

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).***

   Pursuant to the Aviation and Transportation Security Act (ATSA),[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. Section 1557 of the Implementing Recommendations of the 9/11 Commission Act (9/11 Act),[2] recognizes this authority and further requires TSA to take specific actions related to pipeline security.

   Consistent with these authorities and requirements, TSA issued Pipeline Security Guidelines in December 2010 and April 2011, and subsequently updated the Guidelines in March 2018 and April 2021.[3] These voluntary guidelines were developed with the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties. These guidelines recommend the submission of security incident information to TSA, and the implementation of security measures to determine the criticality of pipeline facilities.

   In order to execute its security responsibilities within the pipeline industry, it is important for TSA to have knowledge of potential security incidents and suspicious activity within the mode. TSA visits critical pipeline facilities to collect site-specific information from pipeline operators on facility security policies, procedures, and physical security measures. Information is collected on a Critical Facility Security Review (CFSR) Form. As part of this program, TSA follows up with pipeline operators on the implementation of security improvements and recommendations made during facility visits. During critical facility visits, TSA documents and provides recommendations to pipeline operators to improve the security posture of the reviewed facility. TSA then follows up with pipeline operators via email on the status toward implementation of the recommendations made during the critical facility visits. The follow up is conducted at intervals of 6, 12 and 18 months after the facility visit.

   This ICR covers collection of facility security information during critical facility reviews, using the CFSR Form, and follow-up visits with pipeline operators on their implementation of the security recommendations. While implementation of the security recommendations is generally voluntary, TSA also has mandatory requirements covered by this ICR.

   On May 26, 2021, OMB approved TSA's request for an emergency revision of this information collection, allowing for the institution of mandatory requirements. *See* ICR

[1] Pub. L. 107-71 (115 Stat. 598; Nov. 19, 2001), as codified at 49 U.S.C. 114.

[2] Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007), as codified at 6 U.S.C. 1207(d).

[3] *See* https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf
https://www.tsa.gov/for-industry/surface-transportation.

Reference Number: 202105-1652-002. The revision was necessary to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. TSA issued a Security Directive (SD) applicable to owner/operators of a hazardous liquid and natural gas pipeline or liquefied natural gas facility notified by TSA that their pipeline system or facility is critical.[4] These owner/operators are required to review Section 7 of TSA's 2018 Pipeline Security Guidelines (with Change 1 (April 2021)) and assess current activities, using a TSA-provided form, to address cyber risk, and identify remediation measures that will be taken to fill those gaps and a timeline for achieving those measures. The form provided is based on the instrument used for the CFSRs, limited to cybersecurity issues and augmented to address the scope of the SD.

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.***

<u>Voluntary Collection</u>.
TSA analyzes the information collected on the CFSR form during the onsite facility reviews, as well as the information collected from follow-up with facility operators on the status of recommendations made during the reviews, to determine strengths and weaknesses at the nation's critical pipeline facilities, areas to target for risk reduction strategies, pipeline industry implementation of the TSA "Pipeline Security Guidelines," and the possible need for regulations in accordance with section 1557(d) of the 9/11 Act. TSA is generally the sole user of this information.

<u>Revision to voluntary collection</u>.
TSA is revising the information collection to align the CFSR question set with the revised Pipeline Security Guidelines, and to capture additional criticality criteria. As a result, the question set has been edited by removing, adding and rewriting several questions, to meet the Pipeline Security Guidelines and criticality needs. Further, TSA is moving the collection instrument from a PDF format to an Excel Workbook format. Note that while the criticality information provided by owner/operators is an aspect of TSA's determination of criticality for the mandatory requirements, TSA also considers other information, including intelligence-based risk information.

<u>Mandatory Collection resulting from *Emergency Revision*</u>.
While the above listed collections are voluntary, OMB's emergency approval allowed the revision of the collection to mandate that the owner/operators subject to the requirements of the SD conduct a self-assessment of their cybersecurity using a portion of the previously approved assessment tool. While the currently approved assessment process involves TSA identifying the vulnerabilities identified as part of the assessment and may recommend actions the owner/operator could take to address vulnerabilities, the SD requires owner/operators to identify areas where their practices do not align with the recommendations in the Guidelines and develop a remediation plan. The assessment and identification of gaps must be completed using a Pipeline Cybersecurity Self-Assessment form provided by TSA. TSA uses the results of the assessments to make a global assessment

[4] Under section 1557(b) of the 9/11 Act, TSA is required to identify the 100 most critical pipeline operators. The criteria used to identify these systems and facilities is being used to designate the owner/operators subject to TSA's security directive. Due to the sensitive nature of this information, TSA is individually notifying each Owner/Operator that they are a designated critical operation subject to the security directive's requirements.

of the cyber risk posture of the industry and possibly impose additional security measures as appropriate or necessary. TSA may also use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and Cybersecurity and Infrastructure Security Agency may also use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.

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.***

Voluntary collection: TSA personnel collect facility-specific information on security policies, procedures, and physical security measures on-site using the CFSR Form. TSA personnel complete and finalize the form, then forward it to operators via electronic mail. TSA sends requests to follow up with pipeline operators regarding the status of their implementation of the recommendations made during critical facility visits via electronic mail.

Mandatory collection: Regarding the mandated information collection, owner/operators are required to conduct the assessment of their cybersecurity posture using the TSA Pipeline Cybersecurity Self-Assessment form and submit the results to TSA. There are two methods for owner/operators to submit the required information, which are considered Sensitive Security Information under 49 CFR part 1520 once completed. The first is via email and a password protected document with the password being sent in a separate email. The second is to upload the document on a specific secure portal that TSA has established.

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.***

In some instances, pipeline critical facilities may also fall under the requirements of domestic maritime security regulations required by the Maritime Transportation Security Act of 2002, Public Law 107-295, 116 Stat. 2064 (November 25, 2002) (MTSA). MTSA regulations are enforced by the U.S. Coast Guard and contain specific security requirements for maritime facilities. Many of the maritime security requirements are similar to those TSA would review and under which TSA would collect information during pipeline security reviews. Therefore, TSA asks each operator to identify those pipeline critical facilities that are also MTSA-regulated facilities, and then confirms with the U.S. Coast Guard that the facilities are indeed MTSA-regulated. Upon receiving confirmation from the U.S. Coast Guard, TSA does not review facilities that are MTSA-regulated as security information has already been collected by the U.S. Coast Guard and is available for TSA review as necessary.

Regarding the mandated information collection, no other agency requires submission of cybersecurity assessments 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.***

   There will be no impact on companies that could be considered small businesses. This information request targets the Top 100 most critical pipeline systems in the U.S., and none of the operators of these pipeline systems or their parent companies could be categorized as a small business.

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.***

   Failure to obtain the information from these collections would impact TSA's ability to assess the security posture of the nation's critical pipeline facilities, which will prevent the agency from being able to make specific recommendations to improve each facility's security. The 9/11 Act requires TSA to monitor implementation of security recommendations in order to determine if regulations are required to mitigate risks that are not being addressed. *See* section 1557(d) of the 9/11 Act. Obtaining this information is also necessary for TSA to make company or site-specific recommendations to operators of critical pipeline facilities. Absent this information, the agency will be unable to assess the implementation of security recommendations at a later date, as recommended by the U.S. Government Accountability Office (GAO-10-867, August 2010). In summary, the inability to conduct these collections would greatly impede TSA's mission to protect and secure the nation's hazardous liquid and natural gas pipeline infrastructure.

   Without the mandated collection, DHS will be unable to address the critical threat to the nation's pipeline systems.

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).***

   This collection will be conducted consistent with the 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 <u>Federal Register</u> 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 published a *Federal Register* notice, with a 60-day comment period, soliciting comments on the information collection. *See* 86 FR 34776 (June 30, 2021).

TSA received three (3) comments on the 60-day notice. *See* Supporting Statement Appendix for TSA's response to the comments

TSA also published an additional notice in the Federal Register with a 30-day running period. *See* 86 FR 57197 (October 14, 2021). TSA did not receive any comments on the 30-day notice.

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.

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 that the information provided by operators is Security Sensitive Information, it will be protected in accordance with procedures meeting the transmission, handling, and storage requirements set forth in 49 CFR part 1520. In addition, business contact information is collected and handled pursuant to the DHS/ALL/PIA-006 DHS General Contact Lists PIA to facilitate the assessment of cyber risks and identify remedial measures for critical pipelines.

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.

There are no questions of sensitive nature posed in the collection.

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

TSA estimates the annual burden for the information collection related to the CFSR Form to be 320 hours. TSA estimates a maximum of 80 facility reviews will be conducted each year, with each review taking approximately 4 hours (80 facility reviews x 4 hours = 320 hours).

TSA conducts a follow-up with each reviewed facility operator at 6 months, 12 months, and 18 months after the initial review, for a total of 3 follow-ups per facility operator. TSA estimates it will take approximately 2 hours for each operator to submit a response to TSA regarding its implementation of security recommendations during each follow-up visit, for a total of 6 hours (3 visits x 2 hours). TSA estimates a maximum of 80 critical facilities are reviewed each year, and TSA estimates the total annual burden to be approximately 480 hours (80 CFSR follow ups x 6 hours per follow up).

TSA estimates 100 owner/operators will complete and submit the Pipeline Cybersecurity Self-Assessment form, and it will take each owner/operator 6 hours to complete and submit this form, for a total of 600 hours (100 x 6).

TSA estimates the total estimated annual number of responses is 260 with a total annual burden of 1400 hours. Table 1 displays the total estimated annual hour burden for this ICR.

Table 1: Total Annual Hourly Burden

Collection	Number of Respondents	Hourly Burden	Total Annual Hourly Burden
	A	B	C = A x B
CFSR Form	80	4	320
CFSR Recommendation Follow-up	80	6	480
Pipeline Cybersecurity Self-Assessment Form	100	6	600
Totals	**260**		**1,400**

TSA estimates the total estimated annual hour burden cost for critical pipeline facility owner/operators by utilizing the compensation rates of the owner/operator representatives. TSA assumes each owner/operator will have combination of a corporate security manager, facility manager, and front-line pipeline operator as the representatives during the CFSR form meeting. TSA also assumes only the corporate security manager will be involved with completing responses to TSA for the CFSR follow-ups and the corporate Cybersecurity Coordinator will complete the Cybersecurity Self-assessment. TSA uses a loaded hourly compensation wage of $87.06[5] for each corporate security manager; a loaded hourly compensation wage of $95.07[6] for each pipeline facility manager; a loaded hourly compensation wage of $99.74 for each cybersecurity coordinator;[7] and a loaded hourly compensation wage of $49.42[8] for each front-line pipeline operator.

TSA estimates an hour burden cost of $74,093 for the initial CFSR form meeting. Table 2 displays the calculation of this cost.

Table 2: Hour Burden Cost for CFSR Form

Job Description	Hour Burden	Hourly Wage Rate	Hour Burden Cost

[5] NAICS 486000 – Pipeline Transportation, 11-1021 General and Operations Manager Wage Rate of $61.30 x BLS Compensation Factor of 1.420155039. Compensation Factor is the hourly total compensation of $36.64 divided by the hourly wages, $25.80. BLS wage rate can be found at https://www.bls.gov/oes/2020/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06172021.htm in Table 1. Retrieved July 19,2021.

[6] NAICS 486000 – Pipeline Transportation, 11-3051 Industrial Production Manager Wage Rate of $66.94 x BLS Compensation Factor of 1.420155039. BLS wage rate can be found at https://www.bls.gov/oes/2020/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06172021.htm in Table 1. Retrieved July 19,2021.

[7] NAICS 486000 – Pipeline Transportation, 11-3021 Computer and Information Systems Managers Wage Rate of $70.23 x BLS Compensation Factor of 1.420155039. BLS wage rate can be found at Compensation Factor of 1.420155039. BLS wage rate can be found at https://www.bls.gov/oes/2020/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06172021.htm, Table 1. Retrieved August 17, 2021.

[8] NAICS 486000 – Pipeline Transportation, 17-3020 Engineering Technicians Wage Rate of $34.80 x BLS Compensation Factor of 1.420155039. BLS wage rate can be found at https://www.bls.gov/oes/2020/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06172021.htm, Table 1. Retrieved July 19,2021.

	A	B	C = A x B
Corporate Security Manager	320	$87.06	$27,858
Facility Manager		$95.07	$30,421
Front-line operator		$49.42	$15,815
Total			**$74,093**

Note: Calculations may not be exact due to rounding in table.

TSA estimates an hour burden cost of $41,787 for CFSR recommendation follow-ups for corporate security managers ($87.06 compensation rate x 480 hours).
TSA estimates an hour burden cost of $59,842 for the Cybersecurity Self-assessment for corporate cybersecurity coordinators ($99.74 compensation rate x 600 hours).

TSA estimates a total hour burden cost of $175,743 for this ICR ($74,093 CFSR form cost + $41,787 CFSR form follow-up cost + $59,842).

13. ***Provide an estimate of the total annual cost burden to respondents or record keepers resulting from the collection of information.***

TSA does not estimate a cost to the 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.***

TSA assumes a J-band Surface Transportation Security Specialist (TSS) will represent the agency at each meeting. TSA uses a loaded compensation wage rate of $85.80[9] for the J-band TSS employee. TSA estimates an annual time burden of 320 hours for the TSS employee (80 facility visits x 4 hours per visit). Based on this information, TSA estimates a time burden cost of $27,456 for the J-band employee (320 hours x $85.80 compensation wage). Additionally, TSA assumes a cost for planning and follow-up for a TSS per facility. TSA estimates that the J-band employee will spend 1.5 hours for planning each visit and following up after the visit. TSA multiplies 120 hours (80 facilities x 1.5 hours x 4 (initial visit + 3 follow-ups)) by the loaded compensation wage rate of $85.80 to estimate an additional time burden cost of $41,183. Finally, TSA estimates a time burden to TSA for the Cybersecurity Self-Assessment of 2 hours per self-assessment. TSA multiplies 100 Cybersecurity Self-Assessment respondents by 2 hours by the loaded compensation wage rate of $85.80 to get an hour burden cost of $17,160. The total time burden cost is estimated to be $85,799 ($27,456 + $41,183+ $17,160).

For the contractor expenses, the cost to the Federal government is estimated based on contractor costs per facility visit and an annual travel expense to the government. The costs for the CFSR visits include contractor support services to aid in the conduct of the security reviews and to complete the CFSR Form for each facility visited. TSA estimates each facility visit costs approximately $5,055.37 in contractor expenses. Given that TSA assumes

[9] TSA assumes the loaded hourly wage rate of a J band or GS-14. TSA obtained the loaded wages from TSA's Office of Finance and Administration FY21 Modular Cost. The annual loaded wage rate for a J band (GS 14) was $179,062, and TSA divided by 2,087 hours to estimate a loaded hourly wage of $85.80.

80 CFSR visits per year, TSA estimates the contractor expenses for CFSR visits will be $404,429.60 annually ($5,055.37 x 80 visits). In addition, Federal government travel costs for TSA personnel for the critical facility reviews are estimated to be approximately $41,000 annually. TSA estimates a total annual contracting cost of $445,429.60 as displayed in Table 3.

Table 3: Annual Contracting Costs

Number of CFSR Visits/Year	Cost / CFSR Visit	Annual Travel	Annual Contracting Costs
A	**B**	**C**	**D = (A x B) + C**
80	$5,055.37	$41,000	$445,429.60

TSA estimates a total annualized federal government cost of $531,228.60 ($85,799 total time burden cost + $445,429.60 contractor and travel costs).

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 from the previously reported information; however, TSA is adding the burden estimates related to the previously submitted emergency collection for mandatory submission of cybersecurity assessments and remediation measures.

16. For collections of information for which 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.

Critical facility security information collected on the CFSR Form will not be published.

Critical facility recommendations and implementation status will not be published.

Critical facility cybersecurity assessments will not 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.

TSA is not seeking such approval.

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

TSA is not seeking any exceptions.