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).***

Under the Aviation and Transportation Security Act (ATSA) (Pub. L. 107-71, 115 Stat. 597 (November 19, 2001)), 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." *See* 49 U.S.C. 114(d).

Section 403(2) of the Homeland Security Act (HSA) of 2002 (Pub. L. 107-296, 116 Stat. 2178 (November 25, 2002)) transferred all functions of TSA, including those of the Secretary of Transportation and the Under Secretary of Transportation 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.

The *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11Act) specifically tasked TSA to develop and implement a plan for reviewing the pipeline security plans and inspecting critical facilities of the nation's 100 most critical pipeline systems. *See* sec. 1557 of the 9/11 Act (P. Law 110-53, 121 Stat. 266, 475 (Aug. 3, 2007) (codified at 6 U.S.C. 1207(b)). Operators determined their critical facilities based on guidance and criteria set forth in the Department of Transportation's (DOT) September 5, 2002, "Pipeline Security Information Circular" and April 2011 "Pipeline Security Guidelines."

TSA issued Pipeline Security Guidelines in April 2011 and subsequently update the Guidelines in 2018 and 2021. *See* https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf. These voluntary guidelines, which provide explicit agency recommendations for pipeline industry security practices, 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. Included in the guidelines are recommendations for submission of information to TSA. 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 between approximately 12 and 24 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.

Emergency request

As a result of the recent ransomware attack on one of the Nation's top pipeline supplies and other emerging threat information, TSA is preparing to issue a Security Directive (SD) with requirements for TSA-specified critical pipeline Owner/Operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities.[1] This SD includes three information collections, two of which will be covered by a separate emergency request for revision of OMB control number 1652-0055.[2] In order to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure, TSA is seeking emergency approval to amend this collection, 1652-0050, to require all owner/Operators to review Section 7 of TSA's Pipeline Security Guidelines and assess current activities, using the TSA Pipeline Cybersecurity Self-Assessment form, to address cyber risk, and identify remediation measures that will be taken to fill those gaps and a time frame for achieving those measures. The CP Owner/Operators would be required to report the results of this assessment to TSA within 30 days of issuance of the SD, so that TSA may make a global assessment of the cyber risk posture of the industry.

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.

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," operator implementation of recommendations made during TSA critical facility visits, and the possible need for regulations in accordance with section 1557(d) of the 9/11 Act (codified at 6 U.S.C. 1207(d). TSA is generally the sole user of this information.

---

[1] Under section 1557(b) of the *Implementing Recommendations of the 9/11 Commission Act* Pub. L. 110-53 (121 Stat. 266; Aug. 3, 2007) (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.

[2] Under the SD, TSA will also require TSA-specified Owner/Operators to report cybersecurity incidents and potential cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). Second, the SD will require Owner/Operators 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.

Regarding the emergency request, TSA's security directive is requiring the owner/operators subject to the requirements to 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 the TSA Pipeline Cybersecurity Self-Assessment form provided by TSA. TSA will use the results of the assessments to make a global assessment 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 CISA 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.***

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.

Regarding the emergency request, owner/operators will be required to conduct the assessment of their cybersecurity posture using the TSA Pipeline Cybersecurity Self-Assessment form and submit the results to TSA. There will be two methods for owner/operators to submit the required information, which will be considered Sensitive Security Information (SSI) 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 emergency submission, 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 small businesses.

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 (codified at 6 U.S.C. 1207(d)). 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 emergency approval, DHS will be unable to address the critical threat to the nation's pipeline systems. The use of normal PRA clearance procedures is reasonably likely to result in public harm such that TSA and CISA would be hindered in their ability to address immediate threats to pipeline systems if the SD were not issued in the near future.

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 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 is currently seeking an Emergency Approval of this collection. In light of the ongoing cybersecurity threat, TSA is seeking a waiver to the requirement in 5 CFR 1320.13(d) to publish a Federal Register notice announcing TSA is seeking emergency processing of this ICR. Upon approval of the Emergency Request, TSA will seek public comment on the collection following the normal clearance process providing a 60 and 30 Day commenting period.

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 (SSI), it will be protected in accordance with procedures meeting the transmission, handling, and storage requirements set forth in 49 CFR part 1520. In addition, the information is covered under the Privacy Impact Analysis (PIA), DHS/ALL/PIA-006 General Contact Lists (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.

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 estimates the annual burden for the information collection related to the follow-up on the recommendations made to facility operators to be 400 hours. TSA estimates it will take approximately 5 hours for each operator to submit a response to TSA regarding its implementation of security recommendations made during critical facility visits. TSA estimates a maximum of 80 critical facilities are reviewed each year, and TSA estimates the total annual burden to be approximately 400 hours (80 CFSR follow ups x 5 hours per follow up).

TSA estimates the total estimated annual number of responses is 160 with a total annual burden of 720 hours.

Table 1 displays the total estimated annual hour burden for this ICR.

Table 1: Total Annual Hourly Burden

Collection	Number of Respondents	Number of Responses	Hourly Burden	Total Annual Hourly Burden
	A	**B**	**C**	**D = B x C**
CFSR Form	80	80	4	320
CFSR Recommendation Follow-up	80	80	5	400
Totals	**160**	**160**		**720**

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. TSA uses a loaded hourly compensation wage of $91.63[3] for each corporate security manager; a loaded hourly compensation wage of $76.88[4] for each pipeline facility manager; and a loaded hourly compensation wage of $49.99[5] for each front-line pipeline operator.

[3] NAICS 486000 – Pipeline Transportation, 11-1021 General and Operations Manager Wage Rate of $62.59 x BLS Compensation Factor of 1.463900415. Compensation Factor is the hourly total compensation of $35.28 divided by the hourly wages, $24.10. BLS wage rate can be found at https://www.bls.gov/oes/2016/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06092017.htm in Table 1.

[4] NAICS 486000 – Pipeline Transportation, 11-3051 Industrial Production Manager Wage Rate of $52.52 x BLS Compensation Factor of 1.463900415. BLS wage rate can be found at https://www.bls.gov/oes/2016/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06092017.htm in Table 1.

[5] NAICS 486000 – Pipeline Transportation, 17-3020 Engineering Technicians Wage Rate of $34.15 x BLS Compensation Factor of 1.463900415. BLS wage rate can be found at https://www.bls.gov/oes/2016/May/naics3_486000.htm#11-0000. BLS compensation factor can be found at https://www.bls.gov/news.release/archives/ecec_06092017.htm in Table 1.

TSA estimates an hour burden cost of $69,921 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
	A	**B**	**C = A x B**
Corporate Security Manager	320	$91.63	$29,320
Facility Manager		$76.88	$24,603
Front-line operator		$49.99	$15,998
Total			**$69,921**

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

TSA estimates an hour burden cost of $36,650 for CFSR recommendation follow-ups for corporate security managers ($91.63 compensation rate x 400 hours).

TSA estimates a total hour burden cost of $106,571 for this ICR ($69,921 CFSR form cost + $36,650 CFSR form follow-up cost).

Regarding the emergency request, TSA will submit revised burden estimates for the new assessments in the next renewal for this ICR. These estimates will differ as the scope of the assessment is narrower.

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 $74.78[6] for the J-band TSS employee. TSA estimates an annual hour burden of 320 hours for the TSS employee (80 facility visits x 4 hours per visit). Based on this information, TSA estimates an hour burden cost of $23,930 for the J-band employee (320 hours x $74.78 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 one hour for planning each visit and following up after the visit. TSA multiplies 80 hours by the loaded compensation wage rate of $74.78 to estimate an additional time burden cost of $5,982 (80 facilities x 1 hour per follow-up). TSA estimates the total hour burden cost is $29,912 ($23,930 + $5,982).

[6] 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 FY18 Modular Cost. The annual loaded wage rate for a J band (GS 14) was $155,543.55, and TSA divided by 2,080 hours to estimate a loaded hourly wage of $74.7806.

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 $4,749.43 in contractor expenses. Given that TSA assumes 80 CFSR visits per year, TSA estimates the contractor expenses for CFSR visits will be $379,954 annually ($4,749.43 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 $420,954 for purposes of this ICR. Table 3 displays the annual contracting cost for this ICR.

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	$4,749.43	$41,000	$420,954

TSA estimates a total annualized federal government cost of $450,867 ($29,912 time cost + $420,954 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 mandatory submission of cybersecurity assessments and remediation measures to this collection as described above related to the emergency request.

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.