

INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Operator Security Information

1652-0055

- 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.”

Section 403(2) of the Homeland Security Act (HSA) of 2002 (Pub. L. 107-296, 116 Stat. 2315 (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 Assistant Secretary (then referred to as 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.

Pipeline transportation is a mode over which TSA has jurisdiction. As part of its efforts to enhance the security of the nation’s pipeline systems, TSA issued Pipeline Security Guidelines in April 2011. The 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 document are two 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 contact information for company security managers and knowledge of security incidents and suspicious activity within the mode. Additionally, to facilitate the exchange of security information in a timely fashion, contact data is necessary for pipeline operators’ security operations or control centers.

- 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.**

This voluntary collection is for two categories of information: pipeline operator contact data and security incident/suspicious activity information. TSA will use the operator contact information to provide security-related information to company security managers and/or the security operations or control center. Additionally, TSA may use operator contact information to solicit additional information following a pipeline security incident.

The second category of requested information concerns suspicious activities or security incidents involving pipelines. As the lead Federal agency for pipeline security, TSA desires to be notified of all security incidents involving pipeline facilities or systems. TSA will use

the security incident and suspicious activity information provided by operators for vulnerability identification/analysis and trend analysis. The information, with company-specific data redacted, may also be included in TSA's intelligence-derived reports.

Appendix B of the TSA Pipeline Security Guidelines notes that as the lead Federal agency for pipeline security, TSA desires to be notified of all incidents which are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt. Examples of the types of incidents are provided in the guidelines.

TSA will not use the contact information for solicitation or other unnecessary communication not related to TSA's mission.

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. [Effective 03/22/01, your response must SPECIFICALLY reference the Government Paperwork Elimination Act (GPEA), which addresses electronic filing and recordkeeping, and what you are doing to adhere to it. You must explain how you will provide a fully electronic reporting option by October 2003, or an explanation of why this is not practicable.]***

In compliance with GPEA, a fully electronic reporting option is available for pipeline operators to provide contact and suspicious incident information to TSA. Submission of 24/7 contact information of the pipeline company's primary and alternate security manager, and the telephone number of company's security operations or control center may be done through email to pipelinesecurity@dhs.gov. Information regarding incidents which are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt may be submitted to the Transportation Security Operations Center (TSOC) by email at TSOC.ST@dhs.gov.

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.***

A consolidated listing of contact information for pipeline industry security managers and security operations or control centers is not available. This collection effort will not duplicate the efforts of other agencies.

TSA desires information regarding all incidents that indicate a deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt. The Pipeline Security Guidelines recommend that pipeline companies notify the Transportation Security Operations Center (TSOC) of security incidents and suspicious activities involving their systems.

The National Response Center (NRC) serves as the national point of contact for reporting all oil, chemical, radiological, biological, and etiological discharges into the environment anywhere in the United States and its territories. A limited number of pipeline facilities falling under the provisions of the Maritime Transportation Security Act (MTSA) are required to report suspicious activities to the NRC. Duplicative reporting could occur if an operator chose to make a voluntary report to TSOC in addition to the mandated NRC report. Given the small population of pipeline facilities that are subject to MTSA requirements, TSA does not anticipate a large volume of duplicate reporting to TSOC and NRC. That expectation is based on the actual incident reporting patterns TSA has observed from MTSA regulated pipeline facilities. TSOC has coordinated with the NRC to obtain pipeline incident reports that may be of concern to TSA, in the event that a MTSA-regulated pipeline operator submits a report only to the NRC.

The NRC also receives reportable incidents involving hazardous materials regulated by the Pipeline and Hazardous Materials Administration (PHMSA) of the Department of Transportation under 49 CFR part 191 for natural gas and other gases transported by pipeline and 49 CFR part 195 for liquids transported by pipeline.¹ Although the NRC does accept suspicious activity reports, this reporting is not the type of incident for which reporting is mandated under the pipeline regulations. To the extent that terrorist activity resulted in an incident meeting the reporting criteria of the PHMSA regulations, duplicative reporting could occur should an operator choose to contact both the NRC and TSOC. TSA does not anticipate that this will be a common event.

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 voluntary collection is not expected to have a significant impact on small businesses or other small entities.

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 provide operator contact information to TSA will impede the agency's ability to provide security information to pipeline companies in a timely fashion.

As the lead Federal agency for pipeline security, TSA must maintain situational awareness of the industry in order to execute its security responsibilities. TSOC is TSA's 24/7 coordination center during security incidents. If incident information is not reported, the ability of the TSOC to coordinate any required agency involvement/response to the event may be inhibited.

¹ For purposes of the PHMSA regulations, incidents are primarily related to safety concerns, including: release of hazardous materials that results in death or serious injury, property damage, and unintentional loss as well as events that result in an emergency shutdown and other significant events. See 49 CFR 191.3.

Additionally, if the information were not reported, TSA may not otherwise become aware of the incident, which would affect the ability of the agency to meet its statutory obligation to analyze potential threats across all modes. In turn, loss of this information would reduce the efficacy of the intelligence products developed by TSA for its industry and government partners. Currently, industry suspicious incident reported information is used by TSA for several reports, including the Transportation Security and Industry Report, Pipeline Threat Assessments, and Transportation Intelligence Notes. If the collection of suspicious incident information is not conducted, it may hinder TSA's ability to produce intelligence documents of benefit to the pipeline industry as well as other transportation and government stakeholders.

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 voluntary collection will be conducted consistent with the information collection guidelines.

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.

The requests for pipeline operator contact information and security incident/suspicious activity information collection are contained in the Pipeline Security Guidelines (http://www.tsa.gov/sites/default/files/assets/pdf/Intermodal/tsa_pipeline_sec_guideline_april_2011.pdf). These Guidelines were developed with significant input from pipeline industry stakeholders. Two stakeholder meetings were held to provide industry and government representatives an opportunity to assist in drafting the document. Additionally, the draft document was circulated on several occasions among members of the Pipeline Sector Coordinating Committee and other interested industry and government personnel for additional stakeholder review of the recommended security measures.

TSA published a Federal Register notice, with a 60-day comment period, of the following collection of information on August 16, 2013 (78 FR 50077) and a 30-day notice on December 23, 2013 (78 FR 77484).

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.

TSA assures respondents that the portion of the collection that is deemed Sensitive Security Information will be handled appropriately as described in 49 CFR parts 15 and 1520. Per the Privacy Act of 1974, contact information for pipeline security managers is handled and maintained in accordance with the System of Records Notice for Mailing and Other Lists System DHS/ALL-002 – Department of Homeland Security Mailing and Other Lists System (November 25, 2008, 73 FR 71659). There is no assurance of confidentiality provided to the respondents.

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 are posed.

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

There are approximately 3,000 pipeline companies in the United States. TSA estimates that pipeline operators will require a maximum of 15 minutes to collect, review, and submit primary/alternate security manager and security operations or control center contact information by telephone or email. Assuming the voluntary submission of the requested information by all operators, the potential burden to the public is estimated to be a maximum of 750 hours. (3,000 companies X 15 minutes = 750 hours) Turnover of security personnel would necessitate changes to previously-submitted contact information on an as-occurring basis. Assuming an annual employee turnover rate of 10%, the potential burden to the public is estimated to be a maximum of 75 hours. (3,000 companies X 10% turnover = 300 updates; 300 updates X 15 minutes = 75 hours)

Reporting of pipeline security incidents will occur on an irregular basis. TSA estimates that approximately 40 incidents will be reported annually, requiring a maximum of 30 minutes to collect, review, and submit event information. The potential burden to the public is estimated to be 20 hours. (40 incidents X 30 minutes = 20 hours)

Collection	Number of Respondents	Hour Burden for Collection	Total Burden
Operator Contact Information (Initial)	3000	.25 hours	750 hours
Operator Contact Information (Update)	300	.25 hours	75 hours (annually)
Security Incident	40	.5 hours	20 hours (annually)

Total Annual Burden	845 hours
---------------------	-----------

- 13. Provide an estimate of the total annual cost burden to respondents or recordkeepers resulting from the collection of information. (Do not include the cost of any hour burden shown in Items 12 and 14).**

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.**

There are no additional costs to the Federal Government as a result of this voluntary collection.

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

There has been a decrease in burden due to agency estimates. There is no change in the information being collected.

- 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.**

Pipeline operator security contact information will not be published or shared.

Suspicious activity and security incident information, in redacted form, may be published in TSA intelligence-derived reports, which are distributed to pipeline industry and government stakeholders with a need-to-know.

- 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.