INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Operator Security Information

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 of transportation over which TSA has jurisdiction. The Pipeline Security Division within the Office of Transportation Sector Network Management (TSNM) has the lead within TSA for pipeline matters. In order to execute its security responsibilities within the pipeline industry, this voluntary collection is necessary for TSNM Pipeline 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 required 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 and suspicious activity information. The TSNM Pipeline Security Division 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 incidents which are indicative of a deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt. TSNM Pipeline will use the security incident and suspicious activity information provided by operators for vulnerability identification and analysis and trend analysis. The information, in redacted

form, may also be included in the TSA Office of Intelligence Transportation Suspicious Incident Report (TSIR), an unclassified weekly comprehensive review of suspicious incident reporting related to transportation which is provided to industry and government stakeholders.

Pipeline Security Guidelines in Appendix B notes that as the lead Federal agency for pipleline security, TSA desires to be notified of all incidents which are indicative of 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 be duplicative.

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 draft Pipeline Security Guidelines also indicate that pipeline companies should notify the Transportation Security Operations Center (TSOC) of security incidents and suspicious

activities involving their systems. However, there are currently no requirements for the pipeline industry to report suspicious activity or security incidents to TSA.

Pipeline companies currently reports some incidents to the National Response Center (NRC), which 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. The NRC receives reports of incidents involving hazardous materials regulated by the Department of Transportation under the Federal Hazardous Materials Transportation Laws and reportable under 49 CFR 191 for natural gas and other gases transported by pipeline and 49 CFR 195 for liquids transported by pipeline. While in the past the NRC has voluntarily accepted reports on suspicious activity and maritime security breaches, NRC regulations do not mandate that the pipeline industry report such types of incidents, nor does NRC request voluntary reports related to security incidents.

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.

The 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. This applies to the Pipeline Security Division as well as other transportation modes that may potentially be impacted. Additionally, TSA's Office of Intelligence may not receive the incident information, reducing that office's ability to effectively analyze potential threats across all modes.

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 pipeline operator contact information and security incident and suspicious activity information collection requests are contained in the draft Pipeline Security Guidelines. These Guidelines were developed with significant input from pipeline industry stakeholders. Two separate stakeholder reviews were conducted at the Johns Hopkins University Applied Physics Laboratory in Laurel, MD., the first on August 6-7, 2008 and the second on October 15, 2008. Additionally, the draft document was circulated on several occasions among members of the Pipeline Sector Coordinating Committee and other interested industry personnel.

TSA published a Federal Register notice, with a 60-day comment period, of the following collection of information on July 29, 2009, 74 FR 37723 and a 30 day notice on August 16, 2010, 75 FR 44943. In response to the 60 day notice, TSA has received comments from three pipeline operators and a pipeline industry association. MidAmerican Energy Company and Magellan Midstream Partners, L.P. recommended clarifying the criteria of the incident reporting by specifically indicating that the event involved a deliberate act to disrupt pipeline operations. MidAmerican Energy Company also recommended clarifying the criteria for reporting of suspicious applicants to security-sensitive positions, interpreting this as a requirement for background checks for all applicants. Southwest Gas Corporation noted that multiple agencies request pipeline security incident information. Both Magellan Midstream Partners, L.P. and Southwest Gas Corporation recommended that reporting to the NRC be considered sufficient.

The Interstate Natural Gas Association of America (INGAA) indicated that “suspicious” activity was too subjective to use as a criterion for reporting events and that pipeline operators could face potential civil liability. The Association also expressed concern that TSOC could be overwhelmed by the unnecessary reporting of the theft of company credentials, uniforms, and vehicles. MidAmerican Energy Company echoed that concern, specifically with regard to the theft of credentials. Finally, INGAA recommended that a single point of contact be established for reporting pipeline security incidents.

In response to the comments, TSA will modify the draft Guidelines to specify that reporting is requested for incidents that indicate a deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt. TSA does not concur with the recommendation to report to the NRC or other designated agency in lieu of TSOC. There is to date, no current requirement to report suspicious activity to the NRC or point of contact in

the pipeline industry. Although the NRC sometimes reports incidents to TSA there is no systematic reporting of most incidents with which TSA would be concerned. It is logical that TSA, as the lead Federal agency for transportation security, be responsible for the receipt of any suspicious activity reporting in the transportation domain, including pipelines. The TSOC is a 24-hour watch center manned by trained watch officers responsible for monitoring, analyzing, and coordinating response efforts to a variety to suspicious incidents across the transportation domain.

TSA does not agree with INGAA's comments regarding suspicious activity. It is recognized that the criteria for evaluating an activity as suspicious may vary from company to company. Nevertheless, the submission of information regarding events that may indicate pre-operational activities is of considerable value for threat analysis. INGAA's fear about potential civil liability are misplaced. The guidelines are no regulations and are not enforceable. Similarly, TSA does not agree with the comments regarding theft of company credentials, uniforms, and vehicles with company logos. Theft of these items is an effective way to increase access and decrease scrutiny in furtherance of planning and operations.

The draft Pipeline Security Guidelines request that pipeline operators contact TSOC regarding security incidents or suspicious activity. Other than this email or telephonic contact with TSOC, no action beyond that required by the pipeline operator's security plan is expected.

Additionally, TSA does not agree with MidAmerican Energy Company's comment regarding suspicious applicants. No recommendation for background checks for all applicants is contained in the notification criteria or elsewhere in the Guidelines.

There were no comments specifically addressed to the cost and hour burden of this voluntary information collection.

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 as such, as described in 49 CFR Parts 15 and 1520. Per the Privacy Act of 1974, contact information for pipeline security managers and any personally identifiable information they submit as part of a suspicious activity report, is handled and maintained in accordance with the System of Records Notice for Transportation Security Enforcement System
(December 10, 2004, 69 FR 71828).

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 140 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 70 hours. (140 incidents X 30 minutes = 70 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	140	.5 hours	70 hours (annually)

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.

Not applicable. This is a new voluntary 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.

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

Suspicious activity and security incident information, in redacted form, may be published in the TSA Office of Intelligence Transportation Suspicious Incident Report (TSIR), an unclassified weekly comprehensive review of suspicious incident reporting related to transportation which is provided to industry and government stakeholders.

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.