[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

Intent to Request Renewal From OMB of One Current Public Collection of Information: Pipeline Operator Security Information

AGENCY: Transportation Security Administration, DHS.

ACTION: 60-day Notice.

SUMMARY: The Transportation Security Administration (TSA) invites public comment on one currently approved Information Collection Request (ICR), Office of Management and Budget (OMB) control number 1652-0055, abstracted below that we will submit to OMB for renewal in compliance with the Paperwork Reduction Act (PRA). The ICR describes the nature of the information collection and its expected burden. Specifically, the collection involves the submission of contact information for a pipeline company's primary and alternate security manager and the telephone number of the security operations or control center, as well as data concerning pipeline security incidents.

DATES: Send your comments by [Insert date 60 days after date of publication in the Federal Register].

ADDRESSES: Comments may be e-mailed to TSAPRA@dhs.gov or delivered to the TSA PRA Officer, Office of Information Technology (OIT), TSA-11, Transportation Security Administration, 601 South 12th Street, Arlington, VA 20598-6011.

FOR FURTHER INFORMATION CONTACT: Susan L. Perkins at the above address, or by telephone (571) 227-3398.

SUPPLEMENTARY INFORMATION:

Comments Invited

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.), an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The ICR documentation is available at http://www.reginfo.gov. Therefore, in preparation for OMB review and approval of the following information collection, TSA is soliciting comments to--

(1) Evaluate whether the proposed information requirement is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

(2) Evaluate the accuracy of the agency's estimate of the burden;

(3) Enhance the quality, utility, and clarity of the information to be collected; and

(4) Minimize the burden of the collection of information on those who are to respond, including using appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology.

Information Collection Requirement

Purpose and Description of Data Collection

OMB Control Number 1652-0055; Pipeline Operator Security Information. 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."

In executing its responsibility for modal security, TSA produced the Pipeline Security Guidelines in December 2010 following extensive consultation with its government and industry partners (the document was updated and re-issued in April 2011 following implementation of the National Terrorism Advisory System). Participants in this discussion included industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties. These primary Federal guidelines for pipeline security include recommendations for the voluntary submission of pipeline operator security manager contact information to TSA and the reporting of security incident data to the Transportation Security Operation Center (TSOC).

The Pipeline Security Guidelines recommend that each operator provide TSA with the 24/7 contact information of the company's primary and alternate security manager, and the telephone number of the security operations or control center. Submission of this voluntary information may be done by telephone, email, or any other method convenient to the pipeline operator.

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. The Pipeline Security Guidelines request pipeline operators notify the Transportation Security Operation Center (TSOC) via phone at 866-615-5150 or email at TSOC.ST@dhs.gov as soon as possible if any of

the following incidents occurs or if there is other reason to believe that a terrorist incident may be planned or may have occurred:

- Explosions or fires of a suspicious nature affecting pipeline systems, facilities, or assets;
- Actual or suspected attacks on pipeline systems, facilities, or assets;
- Bomb threats or weapons of mass destruction (WMD) threats to pipeline systems, facilities, or assets;
- Theft of pipeline company vehicles, uniforms, or employee credentials;
- Suspicious persons or vehicles around pipeline systems, facilities, assets, or right-of-way;
- Suspicious photography or possible surveillance of pipeline systems, facilities, or assets;
- Suspicious phone calls from people asking about the vulnerabilities or security practices of a pipeline system, facility, or asset operation;
- Suspicious individuals applying for security-sensitive positions in the pipeline company;
- Theft or loss of Sensitive Security Information (SSI) (detailed pipeline maps, security plans, etc.); and
- Actual or suspected cyber-attacks that could impact pipeline Supervisory Control and Data Acquisition (SCADA) or enterprise associated IT systems.

When contacting the TSOC, the Guidelines request pipeline operators provide as much of the following information as possible:

- Name and contact information (email address, telephone number);

- The time and location of the incident, as specifically as possible;
- A description of the incident or activity involved;
- Who has been notified and what actions have been taken; and
- The names and/or descriptions of persons involved or suspicious parties and license plates as appropriate.

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 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 percent, the potential burden to the public is estimated to be a maximum of 75 hours (3,000 companies x 10 percent turnover = 300 updates; 300 updates x 15 minutes = 75 hours).

TSA expects 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)

Use of Results

The renewal of this information collection will allow TSA to continue using 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. TSA will use the security incident information provided by operators for vulnerability identification and analysis and trend analysis.

Since the 2011 issuance of the Pipeline Security Guidelines, reports of security incidents in the pipeline industry have been routinely used by the TSA to analyze trends in suspicious activities. This analysis is incorporated into TSA's annual pipeline modal threat assessment. TSA may also include incident information, in redacted form, in additional intelligence reports produced by TSA relevant to transportation security. TSA recognizes 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. To the extent that incident information provided by pipeline operators is SSI, it will be protected in accordance with procedures meeting the transmission, handling, and storage requirements of SSI set forth in 49 CFR parts 15 and 1520.

Dated: August 7, 2013

Susan L. Perkins,

TSA Paperwork Reduction Act Officer,

Office of Information Technology.

[FR Doc. 2013-19974 Filed 08/15/2013 at 8:45 am; Publication Date: 08/16/2013]