INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Operator Security Information
1652-0055
Exp. 11/30/2021

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 submission of security incident information to TSA.

In order to execute its security responsibilities within the pipeline industry, TSA needs to have current awareness of potential security incidents and suspicious activity within the mode. Section 227 of the HSA, as amended, established the national cybersecurity and communications integration center (NCCIC) to function as "a Federal civilian interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cybersecurity risks, incidents, analysis, and warnings for Federal and non-Federal entities."[4] Consistent with Homeland Security Presidential Directive (HSPD)-23, the United States Computer Emergency Readiness Team (US-CERT), within the NCCIC, generally functions as the federal information security incident center.[5] The Cybersecurity Information Sharing Act of 2015 requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with certain federal entities in an automated and real-time manner.[6] The US-CERT website is a primary tool used by constituents to report incident information, access information sharing products and services, and interact with US-CERT and its partners within the NCCIC. Constituents, which may include anyone or any entity in the public, use forms located on the website to complete

---

[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).
[3] *See* https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf https://www.tsa.gov/for-industry/surface-transportation.
[4] 6 U.S.C. 659(c)(1).
[5] HSPD-23, at ¶¶ 15, 30.
[6] 6 U.S.C. 1504(c).

these activities. OMB control number 1670-0037 covers voluntary reporting to the Cybersecurity and Infrastructure Security Agency (CISA) through the US-CERT website.

On May 26, 2021, OMB approved TSA's request for an emergency revision of this information collection. *See* ICR Reference Number: 202105-1652-002. The revision was necessary as TSA took action to address the May 2021 ransomware attack on one of the Nation's top pipeline supplies and other emerging threat information. To prevent similar attacks against other pipeline entities, TSA issued 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.[7] The following two information collections included in this SD are covered here.[8] First, TSA now requires all owner/operators subject to the SD's requirements to report cybersecurity incidents or potential cybersecurity incidents on their information and operational technology systems to the CISA within 12 hours of identification of a cybersecurity incident using the CISA Reporting System. Second, the SD requires critical pipeline owner/operators to appoint cybersecurity coordinators, who must be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise, and to provide contact information for the coordinators to TSA. To ensure that information reported pursuant to the SD is identifiable within the system, TSA requires these owners/operators to indicate that they are providing the information pursuant to 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.

Voluntary Collection. As the lead Federal agency for pipeline security, TSA needs to be notified of all security incidents involving pipeline facilities or systems. TSA currently asks pipeline owner/operators to report suspicious activities or security incident data to the TSA Transportation Security Operations Center (TSOC). The scope of the request includes all incidents that are indicative of a possible 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 Pipeline Security Guidelines. The scope of the voluntary reporting applies to any type of security incident affecting the pipeline system or facilities. TSA uses the information voluntarily submitted, including the security incident and suspicious activity information, for vulnerability identification/analysis and trend analysis. The information, with company-specific data redacted, may also be included in TSA's intelligence-derived reports.

Mandatory Collection. OMB approved TSA's emergency request to revise the collection to mandate appointment of a Cybersecurity Coordinator and reporting of cybersecurity incidents for TSA-specified critical pipeline owner/operators of hazardous liquid and natural gas pipelines and liquefied natural gas facilities. Pursuant to the SD, TSA requires pipeline owner/operators to appoint a U.S. Citizen Cybersecurity Coordinator who must submit contact information. The Cybersecurity Coordinator serves as the primary contact for cyber-

[7] 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 SD. 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 SD's requirements.

[8] The additional requirement in the SD to conduct a cybersecurity assessment is covered under a separate OMB control number 1652-0050.

related intelligence information and cybersecurity-related activities and communications with TSA and CISA; must be accessible to TSA and CISA 24 hours a day, seven days a week; must coordinate cyber and related security practices and procedures internally; and must work with appropriate law enforcement and emergency response agencies.

Pipeline owner/operators report actual and potential cybersecurity incidents to CISA within 12 hours of identification of a cybersecurity incident. The information provided to CISA pursuant to the SD is shared with TSA and may also be shared with the National Response Center (NRC) and other agencies as appropriate. Conversely, information provided to TSA pursuant to this directive is shared with CISA and may also be shared with the NRC and other agencies as appropriate.

TSA may also use this information to identify the need to 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 use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information.

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.]

TSA, pursuant to the SD, collects Pipeline Cybersecurity Coordinator contact information, submitted to TSA via email or regular mail.

Cybersecurity incident reports are submitted using the CISA Reporting System form at: . Incident reports can also be reported by calling (888) 282-0870. In compliance with the Government Paperwork Elimination Act, a fully electronic reporting option is available for pipeline operators to provide suspicious incident information to TSA. Information regarding incidents which are indicative of a possible deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt may be submitted to the 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.

This collection effort will not duplicate the efforts of other agencies.

TSA desires information regarding all incidents that indicate a possible deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt. TSA's

Pipeline Security Guidelines recommend that pipeline companies notify the TSOC of security incidents and suspicious activities involving their systems.

The Cybersecurity Information Sharing Act of 2015 requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with certain federal entities in an automated and real-time manner. 6 U.S.C. § 1504(c).

The 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.[9] 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 Safety 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.[10] 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.

For the mandatory requirements, TSA's SD also requires appointment of a cybersecurity coordinator and submission of contact information to TSA. As there is currently no requirement for owner/operators to appoint a cybersecurity coordinator, a consolidated listing of contact information for pipeline Cybersecurity Coordinators is not available. This collection effort will not duplicate the efforts of other agencies.

Cybersecurity incidents and potential cybersecurity incidents are reported to CISA. To avoid duplicate reporting, information provided to CISA pursuant to the SD will be shared with TSA and may also be shared with the NRC and other agencies as appropriate. Similarly, any relevant information provided to TSA pursuant to the directive will be shared with CISA and may also be shared with the NRC and other agencies as appropriate. All reported information will be protected using appropriate system controls.

---

[9] *See* Section 106 of MTSA of 2002 (Pub. L. 107-295, 116 Stat. 2064 (November 25, 2002).

[10] 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.

TSA may use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity 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 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.

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.

With regard to cybersecurity incident reporting pursuant to the SD, it is critical that CISA and TSA are aware of cybersecurity incidents and potential cybersecurity incidents which may impact critical infrastructure and pipeline product delivery. CISA is DHS's 24/7 coordination center for cyber security incidents. If incident information is not reported, the ability of CISA to coordinate any required agency involvement/response to the event may be inhibited. Information received by CISA may be shared with other agencies as necessary to support.

DHS must be able to coordinate cybersecurity incident information quickly and accurately with a pipeline owner/operator. For this reason, TSA must have a point of contact at each critical pipeline company to ensure communication regarding cybersecurity.

Additionally, if the information were not reported, DHS may not otherwise become aware of security incidents, which would affect the ability of the department to meet its statutory obligation to analyze potential cybersecurity threats across all critical infrastructure. In turn, loss of this information would reduce the efficacy of the intelligence products developed by TSA and CISA 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. The Cybersecurity Information Sharing Act of 2015 requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with certain federal entities in an

automated and real-time manner. 6 U.S.C. § 1504(c). If the information is not reported, CISA will not be able to alert other agencies that need the information to identify.

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, except for those in 5 CFR 1320.5(d)(2)(i), which requires respondents to report information to the agency more often than quarterly. Quarterly reporting would not meet the security needs that is the basis for this information collection. DHS needs owner/operators to report cybersecurity incident information as soon as practicable. For required reporting, information must be provided no later than 12 hours after a cybersecurity incident is discovered, or within 12 hours of recognition of a potential cybersecurity incident.

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.

In Security Directive Pipeline-2021-01, Enhancing Pipeline Cybersecurity, TSA provided detailed definitions, requirements and instructions related to cybersecurity incident reporting and the appointment of pipeline Cybersecurity Coordinators.

TSA invited public comment on this information collection requirement, a 60-day notice was published in the *Federal Register* on June 30, 2021 (86 FR 34777) and a 30-day notice was published on October 14, 2021 (86 FR 57198).

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

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.

While there is no assurance of confidentiality provided to Cybersecurity Coordinators, TSA protects information collected from disclosure to the extent appropriate under applicable provisions of the Freedom of Information Act, Federal Information Security Management Act, E-Government Act, and Privacy Act of 1974. TSA would also appropriately treat any

information collected that it determines is Sensitive Security Information and/or Personally Identifiable Information, consistent with the requirements of 49 CFR part 1520 and OMB Guidance, M-07-16.

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. *See* 49 CFR part 1520. In addition, any PII associated with reported incidents is handled in accordance with the System of Records Notices for DHS/TSA-001 Transportation Security Enforcement Record System 79 FR 6609 (February 4, 2014) and; and DHS/TSA 011 - Transportation Security Intelligence Service Files, 75 FR 18867 (April 13, 2010).

For defensive measures and indicators shared under CISA's framework, federal entities are required to apply appropriate controls to protect the confidentiality of cyber threat indicators that contain personal information of a specific individual or information that identifies a specific individual that is directly related to a cybersecurity threat or a use authorized under CISA to the greatest extent practicable. 6 U.S.C. § 1504(b).

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.

Based on previous reporting under OMB approval, TSA anticipates reporting of pipeline security incidents will occur on an irregular basis. TSA estimates that approximately 32 incidents will be reported annually, requiring a maximum of 30 minutes (0.5 hours) to collect, review, and submit event information by the respondent's Corporate Security Manager or equivalent. The annual burden hours are estimated at 16 hours (48 over three years).

TSA expects the mandatory reporting of pipeline cybersecurity incidents to CISA using CISA Reporting System will occur 20 times per year per pipeline operator. Each incident takes approximately 2 hours to gather the appropriate information and submit the report, therefore the annual burden to the public for this task is 100 x 20 x 2 hours = 4,000 hours (12,000 hours over 3 years).

TSA estimates that approximately 100 pipeline owner/operators will report their cybersecurity coordinator and alternate POC information in Year 1, and it will take the pipeline owner/operator approximately 30 minutes (0.50 hour) to do so. Thereafter, TSA estimates 1 pipeline owner/operator will update their cybersecurity coordinator and/or alternate POC information each year due to turnover, and it will take approximately 30 minutes (0.50 hour) to do so. The total burden for this task over three years is (100 x 0.50 hour) + (0.50 hour) + (0.50 hour) = 51 hours, an average of 17 hours per year.

The average total time burden to the public for this information collection request is estimated to be 16 hours + 4,000 hours + 17 hours = 4,033 hours annually (12,099 hours over

3 years). Based on the respondent's Corporate Security Manager's fully-loaded[11] average hourly loaded wage rate of $87.06,[12] TSA estimates an average total cost of $351,095 annually ($1,053,285 over three years). Table 1 summarizes these calculations.

[11] A fully-loaded wage rate account for non-wage components of employee compensation, such as healthcare and retirement benefits.

[12] The unloaded wage rate for an Operations Specialties Manager is $61.30. BLS. May 2020 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 11-1021 General and Operations Managers. Last modified March 31, 2021 (accessed July 19, 2021).

.

TSA calculates a load factor to increase the unloaded wage to account for non-wage compensation. TSA calculates this factor by dividing the total compensation ($36.64) by the wage and salary component ($25.80) of compensation to get a load factor of 1.420155. BLS. Employer Costs for Employee Compensation - March 2021. Table 1. Employer costs per hour worked for employee compensation and costs as a percent of total compensation: private industry workers. Production, transportation and material moving occupations. Last modified June 17, 2021 (accessed July 19, 2021). .

The fully loaded wage rate is calculated by multiplying the unloaded wage rate by the load factor. $102.15 = $67.51 x 1.51305.

INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Operator Security Information
1652-0055
Exp. 11/30/2021

Table 1: Public Time Burden and Cost

Year	Security Incident Responses	Time Burden Per Security Incident Report (Hrs)	Security Incident Reporting Time Burden (Hrs)	Cybersecurity Incident Responses	Time Burden Per Cybersecurity Incident Report (Hrs)	Cybersecurity Incident Report Time Burden (Hrs)	Cybersecurity Manager POC Info Responses	Time Burden Per POC Report (Hrs)	POC Reporting Time Burden (Hrs)	Total Annual Time Burden (Hrs)	Annual Time Burden Cost
	A	B = 0.5	C = A x B	D	E = 2	F = D x E	G	H = 0.5	I = G x H	J = C + F + I	K = J x $87.06
2021	32	0.5	16	2,000	2	4,000	100	0.5	50	4,066	$353,967.68
2022	32		16	2,000		4,000	1		0.5	4,017	$349,658.43
2023	32		16	2,000		4,000	1		0.5	4,017	$349,658.43
Total	96		48	6000		12,000	102		51	12,099	$1,053,284.54
Average	32		16	2000		4,000	34		17	4,033	$351,094.85

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 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.

Based on previous reporting under OMB approval, TSA estimates that approximately 32 security incidents will be voluntarily reported annually to TSOC, requiring a maximum of 30 minutes (0.5 hours) to process the information provided by the respondents. The report is taken and processed by an H-Band TSA employee. The fully-loaded wage rate for an H-Band employee is $43.21.[13] TSA estimates 2,000 cybersecurity incidents will be reported annually to CISA under the SD's requirements, and that it will take a maximum of 30 minutes (0.5 hours) to process these reports. TSA will receive an average of 34 Cybersecurity POC reports, but the time burden to TSA to process the POC information is negligible. The total time burden to government is estimated to be 1,016 hours (3,048 over three years). TSA applies the fully-loaded wage rate of an H-Band employee of $43.21 to estimate the cost of the time burden to government. TSA estimates the total TSA burden to be $43,905 per year ($131,714 over three years). Table 2 summarizes these calculations.

[13] TSA, Office of Finance and Administration, Personnel Modular Cost Data (FY21).

Table 2: Federal Government Time Burden and Cost

Type of Information Reported	Number of Reported Security Incidents	Hour Burden to Process Report	Annual Hour Burden	Annual Hour Burden Cost
	A	B	C = A x B	D = C x $43.21
Security (Non-Cybersecurity) Incidents	32	0.5	16	$691.41
Cybersecurity Incidents	2,000	0.5	1,000	$43,213.22
Cybersecurity POC Info (Year 1)	34	0	0	$0.00
Total	2,066		1,016	$43,904.64
Average	688.67		3,048	$131,713.91

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 from TSA's previously approved emergency request as identified above.

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.

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.