INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Corporate Security Review (PCSR)
OMB control number 1652-0056
Exp.: 01/31/2022

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).***

The Transportation Security Administration (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." 49 U.S.C. 114(d). In addition to carrying out the security responsibilities in paragraph (d), TSA is responsible for "assess[ing] threats to transportation" and "develop[ing] policies, strategies, and plans for dealing with threats to transportation security." 49 U.S.C. 114(f)(2) and (3). Congress has recognized TSA's responsibility for pipeline security by requiring TSA to conduct assessments of pipeline security systems. *See* section 1557 of the Implementing Recommendations of the 9/11 Commission Act, Pub. L. 110-53 (121 Stat. 475; Aug. 3, 2007), *as codified at* 6 U.S.C. 1207.

In order to assess current industry security practices, TSA implemented its Pipeline Corporate Security Review (PCSR) program. The PCSR is a voluntary, face-to-face visit with a Pipeline Owner/Operator during which TSA discusses the company's corporate level security planning and also completes the PCSR Form, which includes 210 questions concerning the Owner/Operator's corporate level security planning, covering security topics such as physical and cyber security, vulnerability assessments, training, and emergency communications. TSA also follows up on the results of each PCSR.

On July 15, 2021, OMB approved TSA's request for an extension of this information collection, allowing for the continued institution of mandatory cybersecurity requirements.[1] This approval is in addition to separate collection requirements associated with TSA Security Directive (SD) Pipeline-2021-01. *See* ICR Reference Number: 1652-0050 and 1652-0055.[2] To protect against the escalating cybersecurity threat, TSA is preparing to revise this SD series to ensure sustainment of the cybersecurity enhancements required by the initial SD in

[1] On July 15, 2021, OMB approved TSA's request for an emergency revision of the ICR. The revision was necessary as a result of actions TSA took to address the ongoing cybersecurity threat to pipeline systems and associated infrastructure. Specifically, on July 19, 2021, TSA issued Security Directive (SD) 2021-02 applicable to Owner/Operators of critical hazardous liquid and natural pipelines and liquefied natural gas facilities. *See* ICR Reference Number: 202107-1652-002. On November 17, 2021, TSA requested an extension of the ICR, which OMB approved on July 26, 2022. *See* ICR Reference Number: 202111-1652-001.

[2] On May 26, 2021, TSA issued SD 2021-01, which included three information collections. OMB control number 1652-0055, includes two of these information collections, requiring Owner/Operators to report cybersecurity incidents to CISA, and 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. OMB control number 1652-0050 contains the remaining information collection, requiring Owner/Operators to conduct a cybersecurity assessment, to address cyber risk, and identify remediation measures that will be taken to fill those gaps and a time frame for achieving those measures.

this series. This revision is based on industry feedback, discussions with cybersecurity experts, and the processing and consideration of alternative measure requests submitted by Pipeline Owner/Operators in response to SD Pipeline 2021-02. These stakeholders requested that TSA eliminate the prescriptive-based requirements and replace them with performance-based requirements, providing more flexibility to Owner/Operators to determine how they can best meet the intended security outcomes.

This SD was issued in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Energy (including the Federal Energy Regulatory Commission), and the Department of Transportation (including the Pipeline and Hazardous Materials Safety Administration). Under 49 U.S.C. 114(*l*)(2),[3] TSA has the authority to issue security directives if the Administrator of TSA determines that a regulation or security directive must be issued immediately in order to protect transportation security. TSA also has authority, at the discretion of the Administrator, to assist another Federal agency in carrying out its authority in order to address a threat to transportation. *See* 49 U.S.C. 114(m).[4]

This information collection is necessary to protect against the ongoing cybersecurity threat to the United States' national and economic security posed by this threat. The requirements in the SD are necessary to protect against operational disruption and severe degradation of necessary capacity in the event that a bad actor attacks industry infrastructure by exploiting weaknesses in cybersecurity, particularly through unprotected connections between Information Technology (IT) and Operational Technology (OT) systems as noted in CISA alerts over since the initial SD was issued.

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 – Pipeline Corporate Security Review (PCSR). As required by 6 U.S.C. 1207, TSA has used the information collected during the PCSR process to determine baseline security standards and areas of security weakness in the pipeline mode. This data and interaction with stakeholders informs the agency's Pipeline Security Guidelines and Pipeline Security Best Practice Observation documents.

Mandatory Collection – Security Directive Requirements. OMB approved TSA's extension request to require Owner/Operators to implement the following collections of information for TSA's SD Pipeline-2021-02 series.

TSA is requesting OMB approval of the information collection within SD Pipeline-2021-02C to respond to the continuing cybersecurity threats. The following table identifies the difference in the requirements between the current SD and this revision.

[3] Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.

[4] 49 U.S.C. 114(m) grants the TSA Administrator the same authority as the Administrator of the Federal Aviation Administration under 49 U.S.C. 106(m), and is applicable to all modes of transportation.

Current SD	**Revised SD**
Implement prescriptive mitigation measures to reduce the risk of compromise from a cyberattack	Establish and implement a TSA-approved Cybersecurity Implementation Plan (CIP) that describes the specific cybersecurity measures employed and the schedule for achieving the performance outcomes in the SD
Develop a Cybersecurity Contingency/Response Plan to reduce the risk of operational disruption or significant business or functional degradation of necessary capacity in the event of a cybersecurity incident	Develop and maintain an up-to-date Cybersecurity Incident Response Plan to reduce the risk of operational disruption, or the risk of other significant impacts on necessary capacity in the event of a cybersecurity incident
Test the effectiveness of the Owner/Operator's cybersecurity practices through an annual architecture design review	Establish a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve device, network and/or system vulnerabilities

The SD requires collection of certain information. The following table compares the current information that needs to be collected with the revision:

Current SD	SD Pipeline-2021-02C
Submit to TSA a certification of completion of each requirement in the SD upon completion. Follow specified procedures if they choose to request to implement alternative measures to the requirements in the SD or seek a waiver based on safety issues or risk of operational disruption if requirements implemented as required.	Submit a Cybersecurity Implementation Plan (CIP) to TSA for approval that identifies how the Owner/Operator will meet the requirements in the SD. Follow specified procedures to amend their Cybersecurity Implementation Plan if there are changes to ownership or control, or changes affecting security.
Submit a Cybersecurity Contingency/Response Plan to TSA upon request.	Submit a Cybersecurity Incident Response Plan to TSA upon request.
Have a third-party conduct an evaluation of the ICS design and architecture and develop and retain a written report of results, to be provided to TSA upon request.	Submit an annual plan to TSA describing the Owner/Operator's Cybersecurity Assessment Program.
Provide records to document compliance upon request of TSA.	Provide records to document compliance upon request of TSA.

More specifically, SD2021-02C requires the following collection of information not required by the previous directive:

Cybersecurity Implementation Plan.

Develop and submit a Cybersecurity Implementation Plan to TSA for approval, and implement the TSA-approved mitigation measures, to achieve performance outcomes that will reduce the risk of compromise, disruption and degradation to pipeline systems and facilities from a cyberattack. The change from prescriptive requirements to an outcome-focused SD requires the Owner/Operators to tell TSA how they will comply. Having this information ensures that TSA and the Owner/Operator have an agreed upon standard against which the Owner/Operator will be inspected for compliance, removing subjectivity from the process. Absent this information, TSA would not be able to effectively ensure compliance with the SD. The SD requires Owner/Operators to submit a request to amend their Cybersecurity Implementation Plan if, after approval, there are changes to the ownership or control of the operation or changes to operations affecting the cybersecurity measures in their approved plan. This requirement replaces information collections in the previous SD related to notifying TSA when requirements in the SD have been completed and information submitted as part of a request for an alternative measure or waiver request.

Cybersecurity Incident Response Plan

The current SD requires Owner/Operators to develop and adopt a Cybersecurity Contingency/Response Plan that includes measures to reduce the risk of operational disruption, or other significant business or functional degradation to necessary capacity, should their pipeline or facility experience a cybersecurity incident and to ensure the resiliency of their operations in the event of a cybersecurity attack. Owners/operators must provide their Cybersecurity Incident Response Plan to TSA upon request. The primary change to this requirement from the current SD is the title of the plan and removal of a specific compliance deadline. The title was changed in response to industry comments.

Cybersecurity Assessment Program

The current SD requires Owner/Operators to have a third-party annually conduct a very specific type of assessment. A written report detailing the results must be provided to TSA upon request and maintained for two years. To reflect comments from industry and cyber experts, TSA is revising this section to replace the prescriptive assessment capability with a requirement for Owner/Operators to have a cybersecurity assessment program that is appropriate for its operations and flexible to address changing dynamics in testing and assessments. SD Pipeline-2021-02C will require the Owner/Operator to provide TSA with annual plan that describes this assessment program. TSA will review the plans and may provide feedback on how it can be improved to address the performance outcomes.

Providing Records to Establish Compliance

The SD Pipeline-2021-02C does not require specific records of compliance to be maintained, but identifies the types of common IT or OT system records TSA may ask to see as part of a compliance inspection. These are all records normally generated by an IT or OT system. If the records are not available or not kept by the Owner/Operator, TSA will work with them to identify other documentation to establish compliance. The requirement to provide records of compliance was in SD Pipeline-2021-02. The revised directive provides some examples of the types of information that could be used to establish compliance and also clarifies that TSA will not always require these records to be submitted. In many situations, providing TSA with access on site will be sufficient.

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.***

Voluntary Collection – Pipeline Corporate Security Review (PCSR).

The voluntary collection of PCSR information is conducted by means of a site visit to a Pipeline Owner/Operator's headquarters location. During the site visit, TSA discusses the Owner/Operator's security planning, and all information captured during the visit is later recorded electronically by TSA onto the PCSR Workbook. This collection workbook is secured and retained electronically by TSA upon completion and used for analysis in determining industry baseline standards. The intent of the PCSR program is to verify that the Owner/Operator is implementing its security program through an onsite review of its security plan as well as to provide a means for TSA to build stakeholder relations through a face-to-face discussion on security planning, a goal which is not readily achievable or practicable if an electronic reporting option were available to the Owner/Operator as an alternative to the onsite visit.

Mandatory Collection – Security Directive Requirements.

Regarding the mandatory collection, TSA requires the following collection of information and maintenance of records to establish compliance with SD 2021-02C:

Cybersecurity Implementation Plan: Pipeline Owner/Operators shall transmit their implementation plans to TSA electronically via a secure means. All implementation plans submitted by operators are considered Sensitive Security Information (SSI) under the provisions of 49 Code of Federal Regulations, part 1520 (49 CFR 1520).

Cybersecurity Incident Response Plan: If requested by TSA, Pipeline Owner/Operators shall transmit their cybersecurity Incident Response plans to TSA electronically via a secure means. All cybersecurity Incident Response plans submitted by operators are considered SSI under the provisions of 49 CFR 1520.

Cybersecurity Assessment Program: Pipeline Owner/Operators shall transmit their cybersecurity assessment plans on an annual basis to TSA electronically via a secure means. All cybersecurity assessment plans submitted by operators are considered SSI under the provisions of 49 CFR 1520.

Records to Establish Compliance: Pipeline Owner/Operators shall provide to TSA electronically, as part of a compliance inspection, documentation to establish their compliance with the SD. Operator records provided to TSA to document compliance with the SD are considered SSI under the provisions of 49 CFR 1520.

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.***

   Voluntary Collection – Pipeline Corporate Security Review (PCSR).

   Regarding the voluntary collection, TSA works closely with its partners at the U.S. Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) to coordinate security initiatives. Since 2006, the two agencies have operated under an annex to the memorandum of understanding (MOU) between DOT and the Department of Homeland Security. This annex specifically addresses the respective roles and responsibilities of TSA and PHMSA as well as coordination processes. There is no other similar information collection currently in place at PHMSA that specifically targets corporate-level security planning and plan implementation in the pipeline mode of transportation.

   Mandatory Collection – Security Directive Requirements.
   Regarding the mandatory submission, TSA developed the requirements in consultation with CISA and in coordination with DOT (including PHMSA) as well as the Department of Energy (including the Federal Energy Regulatory Commission) and other applicable agencies. TSA has determined that no other agency requires submission of the type of information TSA may collect related to its security directives.

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 information collection should not have a significant impact on small businesses or other small entities. While there are over 2,200 Pipeline Owner/Operators in the United States, this collection (both voluntary and mandatory) focuses on the nation's top 100 Pipeline Owner/Operators, primarily determined by energy throughput. These top 100 operators account for 85 percent of all hazardous liquids and natural gas transported in the United States. These companies are often large, corporate operations with business ventures across the world, and as such, employ hundreds if not thousands of employees. By focusing this collection on the most critical Pipeline Owner/Operators in the United States, TSA is aligning its mission and resources with DHS's risk-based security approach.

   The collection of information required by the SD does not have a significant impact on a substantial number of small businesses as the vast majority of these companies are large, corporate operations with business ventures across the world, and as such, employ hundreds if not thousands of employees.

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.***

   Voluntary Collection – Pipeline Corporate Security Review (PCSR).

   If the voluntary PCSR collection were to be discontinued, this would seriously impede TSA's ability to remain current on minimum security standards being employed in the industry, as well as diminish its ability to identify areas of security weakness, two activities that are critical to the agency in carrying out its transportation security mission. Without means of collecting this information, TSA would be unable to confidently identify security gaps and weakness in the pipeline mode and, consequently, would not be able to effectively identify areas to develop programs to better strengthen modal security.

   Mandatory Collection – Security Directive Requirements.

   Without the mandatory collection, TSA will be unable to address the critical threat to the nation's pipeline systems, which is reasonably likely to result in public harm. For example, if an attack occurred against a pipeline and TSA did not have this collection, Pipeline Owner/Operators may not have adequate cybersecurity measures or a cybersecurity response plan in place. These measures decrease the impact of a cybersecurity incident affecting critical infrastructure and increase an operator's awareness of possible vulnerabilities.

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).***

   There are no special circumstances that would require the collection to be conducted in a manner inconsistent with the general 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 to revise 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-day and 30-day commenting period.

   Please see #2 for the efforts that TSA made to consult externally with industry as well as federal partners.

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.***

No assurances of confidentiality were provided to respondents; however, 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 information collected is deemed SSI, TSA will handle as required by 49 CFR 1520. In addition, Privacy Impact Assessment (PIA) coverage is provided under the DHS/ALL/PIA-006 General Contact Lists PIA. (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.***

No personal questions of a sensitive nature will be posed during the information collection.

12. ***Provide estimates of hour and cost burden of the collection of information.***

Voluntary Collection – Pipeline Corporate Security Review (PCSR).
TSA anticipates completing 20 PCSRs annually. Each PCSR places an 8-hour burden on a respondent, and an additional 3 hours to follow-up on results of each PCSR, for an annual hour burden of 11 hours. The annual hour burden for the entire collection is 220 hours. TSA uses a fully-loaded wage rate[5] of $94.67 for a Corporate Security Manager.[6] TSA estimates an annual hour burden cost to the public of $20,832. Table 1 summarizes these results.

Table 1: Annual Costs for Pipeline Corporate Security Reviews (Voluntary – Previously Required)

Activity	Number of Annual Responses	Hour Burden per Response	Annual Hour Burden	Annual Hour Burden Cost

[5] A fully-loaded wage rate accounts for non-salary cost of employee compensation, such as health and retirement benefits.

[6] The unloaded wage rate for a General and Operations Manager is $63.08. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. SOC 11-1021 General and Operations Managers. Last modified March 31, 2022 (accessed June 15, 2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. To load the wage rate, TSA calculates a load factor to inflate the wage rate to account for benefits. The load factor is 1.501098. BLS. Employer Costs for Employee Compensation - December 2021. Table 5. 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 March 18, 2022 (accessed June 15, 2022). https://www.bls.gov/news.release/archives/ecec_03182022.htm. The fully-loaded wage rate is $63.08 × 1.501098 = $94.67.

	A	B	C = A x B	D = C x $94.67
PCSR	20	8	160	$15,150.28
PCSR Re-interview	20	3	60	$5,681.36
Total	40	11	220	**$20,831.64**

Mandatory Collection – Security Directive Requirements.

Cybersecurity Implementation Plan: TSA estimates 100 entities will develop a cybersecurity implementation plan, and the plan will be developed by a team consisting of a cybersecurity manager and 4 cybersecurity analysts/specialists. TSA assumes the team will spend 2 weeks developing the implementation plan; therefore, the time burden for this task will be 5 individuals x 40 hours x 2 weeks, or 400 hours. TSA uses a fully-loaded, blended wage rate of $82.63[7] to estimate a cost for this task to be $3,305,057. This is a one-time collection, and is depicted in Table 2.

Table 2: Costs for Cybersecurity Implementation Plan (Mandatory - NEW)

Activity	Number of Responses	Time Burden per Response	Time Burden	Time Burden Cost
	A	B	C = A x B	D = C x $82.63
Cybersecurity Implementation Plan	100	400	40,000	$3,305,057.39
Total	**100**		**40,000**	**$3,305,057.39**

Cybersecurity Incident Response Plan: TSA estimates 100 entities will provide Incident Response plans annually, and the time burden per response is 80 hours. TSA assumes the cybersecurity Incident Response plan will be developed by a cybersecurity coordinator, and uses a fully-loaded wage rate of $94.06[8] for this requirement. The annual cost for this requirement is depicted in Table 3.

Table 3: Annual Costs for Cybersecurity Incident Response Plan (Mandatory – Previously Required)

Activity	Annual Number of Responses	Time Burden per Response	Annual Time Burden	Annual Time Burden Cost

[7] TSA calculates a blended wage rate for a team consisting of a cybersecurity manager and four cybersecurity analysts. TSA uses the unloaded rate for computer and information systems managers to represent the cybersecurity manager rate, which is $62.66. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 11-3021 Computer and Information Systems Managers. Last modified March 31, 2022 (accessed June 15, 2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. .
TSA uses the unloaded rate for information security analysts to represent cybersecurity analyst rate, which is $53.14. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 15-1212 Information Security Analysts. Last modified March 31, 2021 (accessed June 15,2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. The unloaded, blended rate = ($62.66 x 0.2) + ($53.14 x 0.8) = $55.04. The fully-loaded wage rate is $55.04 x 1.501098 = $82.63.

[8] Per the previous footnote, the unloaded wage rate for a cybersecurity coordinator is $62.66. To get the fully-loaded rate, TSA multiplies this rate by the load factor of 1.501098, so $62.66 x 1.501098 = $94.06.

	A	B	C = A x B	D = C x $94.06
Cybersecurity Incident Response Plan	100	80	8,000	$752,470.37
Total	**100**		**8,000**	**$752,470.37**

Annual Plan for Cybersecurity Assessment Program: TSA estimates 100 entities will conduct annual audits of their cybersecurity measures, and the time burden for submitting an annual audit plan to TSA is 40 hours. TSA believes the preparation and submission of the plan to TSA will be conducted by a corporate Audit/Compliance Manager, and uses a fully-loaded wage rate of $101.19.[9] The annual cost for this requirement is depicted in Table 4.

Table 4: Annual Costs for Cybersecurity Audits Plans of Cybersecurity Measures (Mandatory - NEW)

Activity	Number of Annual Responses	Hour Burden per Response	Annual Hour Burden	Annual Hour Burden Cost
	A	**B**	**C = A x B**	**D = C x $101.19**
Cybersecurity Audit Plan	100	40	4,000	$404,756.05
Total	**100**		**4,000**	**$404,756.05**

Compliance Documentation: TSA estimates 100 entities will conduct cybersecurity compliance documentation, and the time burden for this requirement is 80 hours. TSA believes this task will be performed by the cybersecurity manager, and applies a fully-loaded wage rate of $94.06. The annual cost for this requirement is depicted in Table 5.

Table 5: Annual Costs for Compliance Documentation (Mandatory - NEW)

Activity	Number of Annual Responses	Hour Burden per Response	Annual Hour Burden	Annual Hour Burden Cost
	A	**B**	**C = A x B**	**D = C x $94.06**
Compliance Documentation	100	80	8,000	$752,470.37
Total	**100**	**80**	**8,000**	**$752,470.37**

The total time burden of this information collection is 220 + 8,000 + 4,000 + 8,000 = 20,220 hours annually, plus a one-time burden of 40,000 hours. The time burden cost of this collection is $20,832 + $752,470 +$404,756 + $752,470 = $1,930,528.43 annually, plus a one-time cost of $3,305,097.39. This is depicted in Table 6.

Table 6: Total Costs

	Time Burden (in Hours)	Time Burden Cost
Year 1	60,220	$5,235,585.82 *(Includes One-time*

[9] The unloaded wage rate for Administrative Services Managers is $67.41. BLS. May 2021 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 11-3012 Administrative Services Managers. Last modified March 31, 2021 (accessed June 15,2022). https://www.bls.gov/oes/2021/May/naics3_486000.htm. TSA multiplies this rate by the load factor of 1.501098, so $67.41 x 1.501098 = $101.19.

		Implementation Plan Cost $3,305,057.39)
Year 2	20,220	$1,930,528.43
Year 3	20,220	$1,930,528.43
Total	**100,660**	**$9,096,642.68**
Average	33,553	$3,032,214.23

13. ***Provide an estimate of annualized capital and start-up costs. (Do not include the cost of any hour burden shown in Items 12 and 14).***

TSA does not estimate a cost to the pipeline 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.***

Voluntary Collection – Pipeline Corporate Security Review (PCSR).
A PCSR is conducted by one (1) representative from TSA; either a Senior Analyst (J Band) or a Junior Analyst (I Band). Each review takes approximately 8 hours per employee. Following the review, an additional 32 hours are devoted to completing the form, which is split equally between two analysts, for an annual hour burden of 800 hours. TSA I-Band employees have an average fully-loaded wage rate of $73.95. TSA J-Band employees have an average fully-loaded wage rate of $85.80. TSA uses a simple average wage rate of $80.53 to estimate the hour burden costs, for an annual hour burden cost of $64,422. Table 6 summarizes these estimates.

- **PCSRs Travel Cost**: In addition, TSA also budgets $41,000 for travel costs to support the PCSR process. Therefore, the total costs of the **PCSR to TSA is $105,422 annually.**

Table 7: TSA PCSR Hour Burden and Costs (Voluntary)

Activity	**Number of Annual Responses**	**Hour Burden per Response**	**Annual Hour Burden**	**Annual Hour Burden Cost**
	A	**B**	**C = A x B**	**D = C x $80.53**
TSA conducts PCSR	20	8	160	$12,884.44
PCSR Follow-up	20	32	640	$51,537.77
TSA Travel PSCR				$41,000.00
Total	**40**		**800**	**$105,422.22**

Mandatory Collection – Security Directive Requirements.
For SD2-C there are three elements of the mandatory collection on which TSA conducts reviews and audits and table & summaries these costs.

Table 8: TSA Hour Burden and Costs (Mandatory)

Activity	**Hour Burden**	**Wage Rate**	**First-Year Hour Burden Cost**
	A	**B**	**C = A x B**

TSA review of Implementation Plan (One Time)	3,200	$90.88	$290,825.84
TSA Compliance Inspection	4,800	$73.95	$354,937.09
TSA Travel for Compliance			$410,000.00
TSA Review of Audit Plan	400	$73.95	$29,580.00
Total			**$1,085,342.93**

Implementation Plan Reviews: TSA estimates it will conduct 100 Implementation Plan reviews utilizing a manager and an analyst. This is a one-time review, and the manager will spend 8 hours conducting the review, while the analyst will spend 24 hours. TSA uses a K-band rate of $102.20 for the manager and J-band rate of $87.11 for the analyst. The total cost of implementation plan reviews is 100 x (8 hours x $102.20) + (24 hours x $87.11) = $290,825.84.

Compliance Inspection: TSA estimates it will conduct 100 compliance inspections utilizing two inspectors. Each inspector will spend 24 hours each per inspection, so the total time burden for this activity will be 48 x 100 = 4800 hours. TSA uses an I-band rate of $73.95 for the inspectors. The labor cost of compliance reviews is 4800 x $73.95 = $354,937.09. In addition, TSA expects to spend $410,000 in travel costs; therefore, the total cost for compliance reviews is $764,937.09.

- **Compliance Travel costs**: TSA estimated $410,000 in travel costs to support the compliance inspection process (2 inspector X 100 client reviews per year x $2,050 per review travel cost).

Audit Plan Reviews: TSA estimates it will conduct 100 Audit Plan reviews annually, and it takes an inspector 4 hours to conduct the review. TSA uses an I-band rate of $73.95 for the inspector. The total cost of audit plan reviews is 100 x 4 hours x $73.95 = $29,580.

Total TSA cost = **$1,149,765.15** (total cost of the voluntary collection **$64,422.22** + total cost of the mandatory information **$1,085,342.93**).

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

TSA is making program changes as a result of the collections to be implemented upon issuance of SD Pipeline 2021-01C.

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.***

Voluntary Collection– Pipeline Corporate Security Review (PCSR).

Security information collected during the PCSR will not be published or shared. To the extent information collected via the PCSR process is considered to be SSI, it will be protected from disclosure and publication, and will be handled as described in 49 CFR 1520.

Mandatory Collection – Security Directive Requirements.

Regarding the mandatory collection, no information resulting from the collections under the SD will be published. However, 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.

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.