INFORMATION COLLECTION SUPPORTING STATEMENT

Pipeline Corporate Security Reviews and TSA Security Directive Pipeline-2021-02 series
OMB control number 1652-0056
Exp.: 02/28/2026

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). In addition, Congress has specifically recognized TSA's responsibility for pipeline security. *See, e.g.*, section 1557 of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53 (121 Stat. 475; Aug. 3, 2007), as codified at 6 U.S.C. 1207, requiring TSA to conduct assessments of pipeline security systems. Under 49 U.S.C. 114(*l*)(2)(A),[1] 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).[2]

Voluntary Collection – Pipeline Corporate Security Review.

To assess current industry security practices, TSA implemented its pipeline Corporate Security Review (CSR) program in 2003. The CSR is a voluntary program where TSA conducts a face-to-face visit with a pipeline Owner/Operator to discuss corporate level security planning. As part of this program, TSA personnel completes the CSR Workbook, which includes 150 questions concerning the Owner/Operator's corporate level security planning, covering security topics such as physical security, vulnerability assessments, training, and emergency communications. TSA also follows up on the results of each CSR.

Mandatory Collection – Security Directive Pipeline 2021-02 Series Requirements.

[1] 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 (of Homeland Security).

[2] 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.

In July 2021, TSA issued Security Directive (SD) Pipeline 2021-02, which instituted mandatory cybersecurity requirements to protect transportation security and critical infrastructure. *See* 49 U.S.C. 114(*l*)(2). This SD series 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 (DOT) (including the Pipeline and Hazardous Materials Safety Administration). TSA has issued regular updates to the SD Pipeline-2021-02 series, making minor changes to the information collection requirements.[3]

This information collection, including both voluntary and mandatory collections, is necessary to protect against the ongoing cybersecurity threat to the national and economic security of the United States. The requirements in the SD series are necessary to protect against operational disruption and severe degradation of necessary capacity if a bad actor attacks industry infrastructure by exploiting weaknesses in cybersecurity, particularly through unprotected connections between Information Technology and Operational Technology systems as noted in CISA alerts 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 –CSR. As required by 6 U.S.C. 1207, TSA has used the information collected during the CSR 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 Pipeline 2021-02 Series Requirements.

OMB approved TSA’s request to require Owner/Operators to implement the collections of information for TSA’s SD Pipeline-2021-02 series. The SD Pipeline-2021-02 series requires the following collection of information from owners and operators of a hazardous liquid or natural gas pipeline, or a liquefied natural gas facility notified by TSA that their pipeline system or facility is critical to protect against the ongoing cybersecurity threat to the United States:

- <u>Cybersecurity Implementation Plan (CIP)</u>.

  Develop and submit a CIP 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. 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

[3] *See* ICR Reference Numbers: 202207-1652-001 and 202212-1652-001; SD Pipeline 2021-02, effective July 26, 2021; SD Pipeline 2021-02A, effective December 10, 2021; SD Pipeline 2021-02B, effective December 17, 2021; SD Pipeline 2021-02C, effective July 27, 2022; SD Pipeline 2021-02D, effective July 27, 2023; SD Pipeline 2021-02E, effective July 27, 2024; and SD Pipeline 2021-02F, effective May 3, 2025. (Accessed Jul 2025 at *https://www.tsa.gov/sd-and-ea*.)

would not be able to effectively ensure compliance with the SD. The SD requires Owner/Operators to submit a request to amend their CIP if, after approval, there are changes to the ownership or control of the operation or if there are changes to operations that affect the cybersecurity measures in their approved plan.

- <u>Cybersecurity Incident Response Plan (CIRP)</u>

  Develop and maintain an up-to-date CIRP for Critical Cyber Systems that includes measures to reduce both the risk and duration of an operational disruption or the risk of other significant impacts on business critical functions should the covered pipeline or facility experience a cybersecurity incident. The CIRP must be provided to TSA upon request and ensures that TSA-designated critical pipeline Owner/Operators have updated cybersecurity plans to respond to a cybersecurity incident and minimize operational disruption to critical infrastructure in the United States. The CIRP must include an annual exercise and must identify who (by position) is responsible for implementing the specific measures in the Incident Response Plan and any necessary resources needed to implement the measures.

- <u>Cybersecurity Assessment Plan (CAP)</u>

  Develop a CAP and submit an annual update to TSA for approval that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures and identify and resolve device, network, and/or system vulnerabilities. The CAP must include a cybersecurity architecture review at least once every 2 years and include a schedule for assessing and auditing the cybersecurity measures in the approved CIP. The CAP ensures that TSA-designated Pipeline Owner/Operators are both conducting annual assessments and confirming that the cybersecurity measures they have in place are working. Owner/Operators must also submit to TSA an annual CAP report of the results of assessments conducted in accordance with the Plan.

- <u>Providing Records to Establish Compliance</u>

  The SD Pipeline-2021-02 series does not require specific records of compliance to be maintained but identifies the types of common Information Technology or Operational Technology system records TSA may ask to see as part of a compliance inspection e.g., asset inventories, network diagrams and policy or procedural documents. Owner/Operators must make records necessary to establish compliance with the requirement of the SD Pipeline 2021-02 series available to TSA upon request for inspection and/or copying. TSA may require Owner/Operators to provide specific documentation and access as necessary to establish compliance.

Revision to the name of the OMB control number 1652-0056.

TSA is changing the name of OMB control number 1652-0056 from "*Pipeline Corporate Security Review*" to "*Pipeline Corporate Security Reviews and TSA Security Directive Pipeline-2021-02 series*" to more accurately represent the information collection.

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 – CSR.

The voluntary collection of CSR 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 into the CSR 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 CSR 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 not available to the Owner/Operator as an alternative to the onsite visit.

Usability Testing (UX) Requirement CSR Workbook: TSA completed an UX on the CSR workbook to test the accuracy of the burden. Three pipeline companies participated in the study, all of which completed the Workbook in preparation for a CSR. The CSR Workbook is filled out and submitted electronically and the pipeline operators confirmed that the burden was 8 hours to complete the form and 3 hours for follow-up for a total of 11 hours. As this time burden was greater than the current burden estimate of 9 hours, TSA adjusted the burden.

Overall, the participants found the CSR Workbook easy to navigate and straight forward and believed that the information collected was necessary to assess pipeline physical security. One operator appreciated the level of detail in the questions and indicated they could use it for reference in their own planning. The participants did not provide any recommendations for the improvement of the Workbook.

Mandatory Collection – Security Directive Pipeline 2021-02 Series Requirements.

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

CIP: Pipeline Owner/Operators must provide their CIPs as prescribed by TSA in the Informational Supplement, "*Informational Supplement for TSA's Security Directive Pipeline 2021-02 Series*." All CIPs submitted by Owner/Operators are considered Sensitive Security Information (SSI) under the provisions of 49 Code of Federal Regulations, part 1520 (49 CFR part 1520).

CIRP: If requested by TSA, Pipeline Owner/Operators must transmit their CIRP as prescribed by TSA in the Informational Supplement, "*Informational Supplement for TSA's Security Directive Pipeline 2021-02 Series*." All CIRPs submitted by Owner/Operators are considered SSI under the provisions of 49 CFR part 1520.

CAP: Pipeline Owner/Operators must transmit their CAP and reports on an annual basis as prescribed by TSA in the Informational Supplement, "*Informational Supplement for TSA's Security Directive Pipeline 2021-02 Series*." All CAPs and annual reports submitted by Owner/Operators are considered SSI under the provisions of 49 CFR part 1520.

Records to Establish Compliance: Pipeline Owner/Operators must make records necessary to establish compliance with the requirement of the SD Pipeline 2021-02 series available to TSA upon request for inspection and/or copying. Owner/Operator records provided to TSA to document compliance with the SD are considered SSI under the provisions of 49 CFR part 1520.

UX Requirement – Mandatory Collection – TSA Security Directive 2021-02 Series Requirements: TSA completed an UX to test the accuracy of the burden for the SD 2021-02 Series Requirements i.e., the CIP, CIRP, CAP and Records to Establish Compliance. Three pipeline companies participated in the study. The CIRP requirement was generally not a burden as most operators has already established cyber security response plans in place. In general, participants found that the first submission of the CIP, CAP, and Records to Establish Compliance between 2021 and 2023 often required multiple revisions and re-submissions before TSA approval. This was due to confusion on the TSA requirements and the level of detail required in the requirements. TSA has resolved these issues with operators through multiple one-on-one engagements. All pipeline operators subject to the collection requirements have approved CIPs and CAPs in place (TSA does not approve the CIRP). The current collection burden is only to maintain and update these documents and, as appropriate, submit them to TSA for approval.

CIP: Pipeline operators confirmed that the burden i.e., approximately 400 hours annually to keep the CIP updated and submit changes for TSA approval was accurate. This included a cybersecurity manager and four analysts (five personnel) spending 2 weeks (80 hours) to update the CIP. Operators noted that the TSA Frequently Asked Questions document was helpful in completing the CIP.

CIRP: Pipeline operators confirmed that the burden i.e., approximately 80 hours annually to keep the CIRP updated was accurate. This included a cybersecurity manager (one person) spending 2 weeks (80 hours) to update the CIP.

CAP: Pipeline operators confirmed that the burden i.e., approximately 160 hours annually to submit a CAP to TSA for approval and submit an annual report was more than the current TSA estimate. This included a cybersecurity manager and an audit compliance manager (two personnel) spending an average of 2 weeks (80 hours) developing and submitting the plan and report. As such, TSA significantly increased the burden from our initial estimate of 40 hours based on this assessment.

Records to Establish Compliance: Pipeline operators confirmed that the burden i.e., approximately 160 hours annually to maintain records to establish compliance was more than the current TSA estimate. This included a cybersecurity manager and an audit/compliance manager (two personnel) spending an average of 2 weeks (80 hours) updating compliance documentation. As such, TSA significantly increased the burden from our initial estimate of 80 hours based on this assessment.

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 – CSR.

   Regarding the voluntary collection, TSA works closely with its partners at the 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 between DOT and the Department of Homeland Security (DHS). 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 Pipeline 2021-02 Series 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 Pipeline-2021-02 series 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 – CSR.

If the voluntary CSR 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 Pipeline 2021-02 Series 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 Owner/Operator's awareness of possible vulnerabilities. The mandatory collection helps TSA identify and respond to the cyber threat more quickly by analyzing patterns across the industries. It also improves government and pipeline operator coordination and information sharing which helps prioritize cyber response and resources.

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 published a 60-day notice, as required by 5 CFR 1320.8(d), in the *Federal Register* on August 1, 2025 (90 FR 36169) and a 30-day notice on January 2, 2025 (91 FR 149). TSA received no comments.

   TSA has collaborated with the pipeline industry to accurately assess the burden on operators for both the voluntary (CSR) measures and the mandatory (TSA SD Pipeline 2021-02 Series) requirements. As the voluntary CSR program has included 21 engagements per year for over a decade, TSA has been able to confirm with operators the accuracy of the cost and time hour burden. However, the cost and time hour burden for the mandatory SD Pipeline 2021-02 Series has been more difficult to assess as the cybersecurity requirements were new in 2021 and TSA intentionally allowed pipeline operator flexibility in determining how to satisfy the cybersecurity measures. In addition, pipeline operators are at different levels of cybersecurity maturity, which affects level of effort necessary to meet TSA's requirements, and therefore there was a large difference in burden between operators. TSA has worked one-on-one with operators to assist them in the development of their CIPs, CAPs, and Records to establish compliance, which have all been approved by TSA. Based on these interactions with 100 pipeline operators, TSA is confident in our estimate of the annual cost and time burden to keep these documents up to date.

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 – CSR.

TSA anticipates completing 21 pipeline CSRs annually. Each pipeline CSR places an 8-hour burden on a respondent, and an additional 3 hours to follow-up on results of each pipeline CSR, for an annual hour burden of 11 hours. The annual hour burden for the entire collection is 231 hours. TSA uses a fully-loaded wage rate[4] of $114.09 for a Corporate

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

Security Manager.[5] TSA estimates an annual hour burden cost to the public of $26,354. Table 1 summarizes these results.

Table 1: Annual Costs for CSR (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 $114.09**
CSR	21	8	168	$19,166.79
CSR Re-interview	21	3	63	$7,187.55
Total	42	11	231	$26,354.33
3-Year Total	**126**	**33**	**693**	**$79,063.00**

Mandatory Collection – Security Directive Requirements.

CIP: All designated Pipeline Owner/Operators have submitted and approved CIPs. TSA estimates that 100 entities will continue to update their CIPs and submit changes to TSA for approval as necessary as cyber controls are updated or changed. The burden is therefore the estimated time annually to keep the CIP current and provide changes to TSA for approval as necessary. TSA estimates updates to the CIP will be conducted by a team consisting of a cybersecurity manager and four cybersecurity analysts/specialists. TSA assumes the team will spend 2 weeks updating 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 $86.48[6] to estimate a cost for this task to be $3,459,002, as depicted in Table 2.

Table 2: Costs for CIP (Mandatory)

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

[5] The unloaded wage rate for a General and Operations Manager is $77.75. BLS. May 2024 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. SOC 11-1021 General and Operations Managers. Last modified April 2, 2025 (accessed April 2025). https://www.bls.gov/oes/2024/may/oessrci.htm#48-49. To load the wage rate, TSA calculates a load factor to inflate the wage rate to account for benefits. The load factor is 1.467370. BLS. Employer Costs for Employee Compensation - December 2024. 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 14 2025 (accessed April 2025). https://www.bls.gov/news.release/archives/ecec_03142025.htm. The fully-loaded wage rate is $77.75 × 1.467370 = $114.09.

[6] 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 $82.10. BLS. May 2024 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 11-3021 Computer and Information Systems Managers. Last modified April 2, 2025 (accessed April 2025). https://www.bls.gov/oes/2024/may/oessrci.htm#48-49. TSA uses the unloaded rate for information security analysts to represent cybersecurity analyst rate, which is $53.14. BLS. May 2024 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 15-1211 Computer Systems Analysts. Last modified April 2, 2025 (accessed April 2025). https://www.bls.gov/oes/2024/may/oessrci.htm#48-49. The unloaded, blended rate = ($82.10 x 0.2) + ($53.14 x 0.8) = $58.93. The fully-loaded wage rate is $58.93 x 1.467370 = $86.48.

		Response		
	A	B	C = A x B	D = C x $86.48
CIP	100	400	40,000	$3,459,002.11
Total	**100**		**40,000**	**$3,459,002.11**

CIRP: All designated Pipeline Owner/Operators have established CIRPs. TSA estimates 100 entities will update their CIRP annually. TSA assumes one cybersecurity manager will spend 2 weeks updating the CIRP; therefore, the time burden for this task is 80 hours. TSA uses a fully-loaded wage rate of $120.47[7] for this requirement. The annual cost for this requirement is depicted in Table 3.

Table 3: Annual Costs for CIRP (Mandatory)

Activity	Annual Number of Responses	Time Burden per Response	Annual Time Burden	Annual Time Burden Cost
	A	B	C = A x B	D = C x $120.47
CIRP	100	80	8,000	$963,768.66
Total	**100**		**8,000**	**$963,768.66**

CAP: All designated Pipeline Owner/Operators have a TSA approved CAP. TSA estimates 100 entities will submit an annual plan for their CAP and an annual report. TSA estimates that two people, a cybersecurity manager and an audit compliance manager will spend an average of 2 weeks developing and submitting the plan and report; therefore, the time burden for this task is 160 hours. TSA uses a fully-loaded wage rate of $97.40.[8] The annual cost for this requirement is depicted in Table 4.

Table 4: Annual Costs for CAP (Mandatory)

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 $97.40
CAP	100	160	16,000	$ $1,558,464.40
Total	**100**		**16,000**	**$ $1,558,464.40**

[7] Per the previous footnote, the unloaded wage rate for a cybersecurity coordinator is $82.10. To get the fully-loaded rate, TSA multiplies this rate by the load factor of 1. 467370, so $82.10 x 1. 467370 = $120.47.

[8] TSA calculates a blended wage rate for the Audit Manager and the Cybersecurity Manager. The unloaded wage rate for the Audit Manager is $50.66. The unloaded wage rate for the Cybersecurity Manager is $82.10. BLS. May 2024 National Industry-Specific Occupational Employment and Wage Estimates. NAICS 486000 - Pipeline Transportation. OCC 11-3012 Administrative Services Managers and OCC 11-3021 Computer and Information Systems Managers. Last modified April 2, 2025 (accessed April 2025). https://www.bls.gov/oes/2024/may/oessrci.htm#48-49. The unloaded, blended rate = ($50.66 x 0.5) + ($82.10 x 0.5) = $66.38. The fully -loaded wage rate is $66.38 x 1. 467370 = $97.40.

Compliance Documentation: TSA estimates 100 entities will work to ensure compliance documentation is kept up-to-date. TSA estimates that two people, a cybersecurity manager and an audit/compliance manager will spend an average of 2 weeks updating compliance documentation; therefore, the time burden for this requirement is 160 hours. TSA applies a fully-loaded wage rate of $97.40. The annual cost for this requirement is depicted in Table 5.

Table 5: Annual Costs for Compliance Documentation (Mandatory)

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 $97.40**
Compliance Documentation	100	160	16,000	$ $1,558,464.40
Total	**100**	**160**	**16,000**	**$** $1,558,464.40

The total time burden of this information collection is 231 + 40,000 + 8,000 + 16,000 + 16,000 = 80,231 hours annually. The time burden cost of this collection is $26,354 + $3,459,002 + $963,769 +$1,558,464 + $1,558,464 = $7,566,054 annually. This is depicted in Table 6.

Table 6: Total Costs

	Time Burden (in Hours)	**Time Burden Cost**
Year 1	80,231	$7,566,054
Year 2	80,231	$7,566,054
Year 3	80,231	$7,566,054
Total	**240,693**	**$22,698,162**
Average	80,231	$7,566,054

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 – CSR.

A CSR is conducted with two individuals from TSA; a Senior Analyst (J Band) and 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 $88.39. TSA J-Band employees have an average fully-loaded wage rate of $104.17. TSA uses a simple average wage rate of $96.28 to estimate the hour burden costs, for an annual hour burden cost of $77,025. Table 7 summarizes these estimates.

- **CSRs Travel Cost**: In addition, TSA also budgets $41,000 for travel costs to support the pipeline CSR process. Therefore, the total costs of the **CSR to TSA is $138,051 annually.**

Table 7: TSA CSR 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 $96.28**
TSA conducts CSR	21	16	336	$32,350.43
CSR Follow-up	21	32	672	$64,700.86
TSA Travel CSR				$41,000.00
Total			**1,008**	$138,051.29

Mandatory Collection – Security Directive Requirements.

For the SD Pipeline 2021-02 series, 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	3,200	$113.22	$347,836.86
TSA Compliance Inspection	4,800	$88.39	$ $424,261.04
TSA Travel for Compliance			$410,000.00
TSA Review of Audit Plan	400	$88.39	$ **$35,356.00**
Total			**$1,217,453.91**

Implementation Plan Reviews: TSA estimates it will conduct 100 Implementation Plan reviews utilizing a manager and an analyst. The manager will spend 8 hours conducting the review, while the analyst will spend 24 hours. TSA uses a K-band rate of $122.27 for the manager and J-band rate of $104.17 for the analyst. The total annual cost of implementation plan reviews is 100 x (8 hours x $122.27) + (24 hours x $104.17) = $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 $88.39 for the inspectors. The labor cost of compliance reviews is 4800 x $88.39 = $424,261.04. In addition, TSA expects to spend $410,000 in travel costs; therefore, the total cost for compliance reviews is $834,261.04.

- **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).

CAP 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 $88.39 for the inspector. The total cost of audit plan reviews is 100 x 4 hours x $88.39 = $35,356.

Total TSA cost = **$1,355,505.20** (total cost of the voluntary collection **$138,051.29**+ total cost of the mandatory information **$1,217,453.91**).

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

As a result of the UX, TSA adjusted the annual time burden for the voluntary collection from 9 hours to 11 hours. TSA also adjusted the annual time burden for the mandatory collection. In particular, TSA increased the burden estimates for the CAP collection from 40 hours to 160 hours and for the Records Compliance from 80 hours to 160 hours.

Also, TSA is changing the name of OMB control number 1652-0056 from "*Pipeline Corporate Security Review*" to "*Pipeline Corporate Security Reviews and TSA Security Directive Pipeline-2021-02 series*" to more accurately represent the information 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.

Voluntary Collection – CSR.

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

Mandatory Collection – Security Directive Requirements.

Regarding the mandatory collection, TSA will not publish any information resulting from the collections under the SD series. 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.