



PRIVACY THRESHOLD ANALYSIS (PTA)

This form serves as the official determination by the DHS Privacy Office to identify the privacy compliance requirements for all Departmental uses of personally identifiable information (PII).

A Privacy Threshold Analysis (PTA) serves as the document used to identify information technology (IT) systems, information collections/forms, technologies, rulemakings, programs, information sharing arrangements, or pilot projects that involve PII and other activities that otherwise impact the privacy of individuals as determined by the Chief Privacy Officer, pursuant to Section 222 of the Homeland Security Act, and to assess whether there is a need for additional Privacy Compliance Documentation. A PTA includes a general description of the IT system, information collection, form, technology, rulemaking, program, pilot project, information sharing arrangement, or other Department activity and describes what PII is collected (and from whom) and how that information is used and managed.

Please complete the attached Privacy Threshold Analysis and submit it to your component Privacy Office. After review by your component Privacy Officer the PTA is sent to the Department's Senior Director for Privacy Compliance for action. If you do not have a component Privacy Office, please send the PTA to the DHS Privacy Office:

Senior Director, Privacy Compliance
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
Tel: 202-343-1717

PIA@hq.dhs.gov

Upon receipt from your component Privacy Office, the DHS Privacy Office will review this form and assess whether any privacy compliance documentation is required. If compliance documentation is required – such as Privacy Impact Assessment (PIA), System of Records Notice (SORN), Privacy Act Statement, or Computer Matching Agreement (CMA) – the DHS Privacy Office or component Privacy Office will send you a copy of the relevant compliance template to complete and return.



Privacy Threshold Analysis (PTA)

Specialized Template for Information Collections (IC) and Forms

The Forms-PTA is a specialized template for Information Collections and Forms. This specialized PTA must accompany all Information Collections submitted as part of the Paperwork Reduction Act process (any instrument for collection (form, survey, questionnaire, etc.) from ten or more members of the public). Components may use this PTA to assess internal, component-specific forms as well.

Form Number:	N/A		
Form Title:	N/A		
Component:	Transportation Security Administration (TSA)	Office:	Security Policy and Industry Engagement (SPIE)

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	Pipeline Operator Security Information		
OMB Control Number:	1652-0055	OMB Expiration Date:	July 31, 2019
Collection status:	Extension	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	Nathan Beam		
Office:	SPIE	Title:	Click here to enter text.
Phone:	571-227-1358	Email:	Nathan.beam@tsa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Christina A. Walsh		
Office:	IT	Title:	Program Specialist
Phone:	571-227-2062	Email:	Christina.walsh@tsa.dhs.gov



SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form	
<p>a. Describe the purpose of the information collection or form. <i>Please provide a general description of the project and its purpose, including how it supports the DHS mission, in a way a non-technical person could understand (you may use information from the Supporting Statement).</i></p> <p><i>If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.</i></p>	
<p>1652-0055 covers the voluntary reporting of suspicious activities or security incident data by pipeline industry representatives to TSA’s Transportation Security Operations Center (TSOC) as prescribed in TSA’s Pipeline Security Guidelines available at https://www.tsa.gov/for-industry/surface-transportation. The TSOC will collect the name and contact information (company, phone number, email address) of the reporter.</p>	
<p>b. List the DHS (or component) authorities to collect, store, and use this information. <i>If this information will be stored and used by a specific DHS component, list the component-specific authorities.</i></p>	
<p>ATSA, Pub. L. 107-71 (Nov. 19, 2001); 49 U.S.C. § 114(d); Pipeline Security Guidelines</p>	

2. Describe the IC/Form	
<p>a. Does this form collect any Personally Identifiable Information” (PII¹)?</p>	<p><input checked="" type="checkbox"/> Yes</p> <p><input type="checkbox"/> No</p>
<p>b. From which type(s) of individuals does this form collect information? (Check all that apply.)</p>	<p><input checked="" type="checkbox"/> Members of the public</p> <p style="padding-left: 20px;"><input checked="" type="checkbox"/> U.S. citizens or lawful permanent residents</p> <p style="padding-left: 20px;"><input checked="" type="checkbox"/> Non-U.S. Persons.</p> <p><input type="checkbox"/> DHS Employees</p> <p><input type="checkbox"/> DHS Contractors</p> <p><input type="checkbox"/> Other federal employees or contractors.</p>

¹ Personally identifiable information means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



<p>c. Who will complete and submit this form? (<i>Check all that apply.</i>)</p>	<p><input type="checkbox"/> The record subject of the form (e.g., the individual applicant).</p> <p><input type="checkbox"/> Legal Representative (preparer, attorney, etc.).</p> <p><input checked="" type="checkbox"/> Business entity. If a business entity, is the only information collected business contact information? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p> <p><input type="checkbox"/> Law enforcement.</p> <p><input type="checkbox"/> DHS employee or contractor.</p> <p><input type="checkbox"/> Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i> Click here to enter text.</p>
<p>d. How do individuals complete the form? <i>Check all that apply.</i></p>	<p><input type="checkbox"/> Paper.</p> <p><input type="checkbox"/> Electronic. (ex: fillable PDF)</p> <p><input type="checkbox"/> Online web form. (available and submitted via the internet) <i>Provide link:</i> Individuals call or email the TSOC.</p>
<p>e. What information will DHS collect on the form? <i>List all PII data elements on the form. If the form will collect information from more than one type of individual, please break down list of data elements collected by type of individual.</i></p>	
<p>The TSOC will collect the name and contact information (company, phone number, email address) of the reporter.</p> <p>TSA requests that the following also be included in incident reporting: • The time and location of the incident, as specifically as possible; • A description of the incident or activity involved; • Which entities have been notified and what actions have been taken; • The names and/or descriptions of persons involved or suspicious parties and license plates as appropriate. The collection of the incident information is covered by DHS/TSA/PIA-029, Operations Center Incident Management System.</p>	



Appendix B of the TSA Pipeline Security Guidelines available at <https://www.tsa.gov/for-industry-/surface-transportation>, notes that as the lead Federal agency for pipeline security, TSA desires to be notified of all incidents which are indicative of a possible deliberate attempt to disrupt pipeline operations or activities that could be precursors to such an attempt.

f. Does this form collect Social Security number (SSN) or other element that is stand-alone Sensitive Personally Identifiable Information (SPII)? *Check all that apply.*

- | | |
|---|--|
| <input type="checkbox"/> Social Security number | <input type="checkbox"/> DHS Electronic Data Interchange Personal Identifier (EDIPI) |
| <input type="checkbox"/> Alien Number (A-Number) | <input type="checkbox"/> Social Media Handle/ID |
| <input type="checkbox"/> Tax Identification Number | <input type="checkbox"/> Known Traveler Number |
| <input type="checkbox"/> Visa Number | <input type="checkbox"/> Trusted Traveler Number (Global Entry, Pre-Check, etc.) |
| <input type="checkbox"/> Passport Number | <input type="checkbox"/> Driver's License Number |
| <input type="checkbox"/> Bank Account, Credit Card, or other financial account number | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Other. <i>Please list:</i> | |

g. List the **specific authority** to collect SSN or these other SPII elements.

N/A

h. How will this information be used? What is the purpose of the collection? Describe **why** this collection of SPII is the minimum amount of information necessary to accomplish the purpose of the program.

N/A

i. Are individuals provided notice at the time of collection by DHS (*Does the records subject have notice of the collection or is form filled out by third party*)?

- Yes. Please describe how notice is provided.
Individuals voluntarily provide incident reporting to TSA by calling or emailing the TSOC.
- No.



3. How will DHS store the IC/form responses?	
a. How will DHS store the original, completed IC/forms?	<input type="checkbox"/> Paper. Please describe. Click here to enter text. <input checked="" type="checkbox"/> Electronic. Please describe the IT system that will store the data from the form. WebEOC <input type="checkbox"/> Scanned forms (completed forms are scanned into an electronic repository). Please describe the electronic repository. Click here to enter text.
b. If electronic, how does DHS input the responses into the IT system?	<input checked="" type="checkbox"/> Manually (data elements manually entered). Please describe. Click here to enter text. <input type="checkbox"/> Automatically. Please describe. Click here to enter text.
c. How would a user search the information submitted on the forms, <i>i.e.</i> , how is the information retrieved?	<input type="checkbox"/> By a unique identifier. ² <i>Please describe.</i> If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. Click here to enter text. <input checked="" type="checkbox"/> By a non-personal identifier. <i>Please describe.</i> Incident number; location; "pipeline"
d. What is the records retention schedule(s)? <i>Include the records schedule number.</i>	Security program records are permanent. Cut off at end of calendar year. Transfer to FRC 3 years after cutoff. Transfer to NARA 10 years after cutoff. In accordance with NARA authority, N1-560-04-10 Item 3.

² Generally, a unique identifier is considered any type of "personally identifiable information," meaning any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.



<p>e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?</p>	<p>The program office's records liaison is responsible for ensuring the regular review of and archival of eligible records.</p>
<p>f. Is any of this information shared outside of the original program/office? <i>If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?</i></p>	
<p><input type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text.</p> <p><input checked="" type="checkbox"/> Yes, information is shared <i>external</i> to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe. TSA may also share information with federal, state, or local law enforcement or intelligence agencies or other organizations in accordance with the Privacy Act and the routine uses identified in the TSOC-applicable Privacy Act system of records notices (SORNs).</p> <p><input type="checkbox"/> No. Information on this form is not shared outside of the collecting office.</p>	



Please include a copy of the referenced form and Privacy Act Statement (if applicable) with this PTA upon submission.



PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	Jennifer L. Schmidt
Date submitted to component Privacy Office:	December 3, 2018
Date submitted to DHS Privacy Office:	December 3, 2018
Have you approved a Privacy Act Statement for this form? <i>(Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.)</i>	<input type="checkbox"/> Yes. Please include it with this PTA submission. <input checked="" type="checkbox"/> No. Please describe why not. Records are not retrieved by a unique personal identifier.
Component Privacy Office Recommendation: <i>Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.</i>	
TSA Privacy recommends approval of this PTA. Collection of PII from members of the public (pipeline industry representatives) is covered by DHS/ALL/PIA-006, DHS General Contacts. SORN coverage is not required. (PIA/SORN coverage for incident reporting and the collection/retrieving of available PII therein is provided by DHS/TSA/PIA-029, Operations Center Incident Management System; DHS/TSA/SORN-001, Transportation Security Enforcement Record System and DHS/TSA/SORN-011 Transportation Security Intelligence Service Files.)	



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Sean McGuinness
PCTS Workflow Number:	1173057
Date approved by DHS Privacy Office:	December 17, 2018
PTA Expiration Date	December 17, 2021

DESIGNATION

Privacy Sensitive IC or Form:	Yes If “no” PTA adjudication is complete.
Determination:	<input type="checkbox"/> PTA sufficient at this time. <input type="checkbox"/> Privacy compliance documentation determination in progress. <input type="checkbox"/> New information sharing arrangement is required. <input type="checkbox"/> DHS Policy for Computer-Readable Extracts Containing SPII applies. <input type="checkbox"/> Privacy Act Statement required. <input checked="" type="checkbox"/> Privacy Impact Assessment (PIA) required. <input checked="" type="checkbox"/> System of Records Notice (SORN) required. <input type="checkbox"/> Specialized training required. <input type="checkbox"/> Other. Click here to enter text.
DHS IC/Forms Review:	DHS PRIV has not received this ICR/Form.
Date IC/Form Approved by PRIV:	Click here to enter a date.
IC/Form PCTS Number:	Click here to enter text.
Privacy Act Statement:	Choose an item. A Privacy Act Statement is not required as information is not retrieved via personal identifier. Records are retrieved by incident number; location; “pipeline”



PTA:	No system PTA required. Click here to enter text.
PIA:	Choose an item. If covered by existing PIA, please list: DHS/ALL/PIA-006 DHS General Contacts and DHS/TSA/PIA-029 Operations Center Incident Management System If a PIA update is required, please list: Click here to enter text.
SORN:	Choose an item. If covered by existing SORN, please list: DHS/TSA-001 Transportation Security Enforcement Record System and DHS/TSA-011 Transportation Security Intelligence Service Files If a SORN update is required, please list: Click here to enter text.
DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i>	
<p>DHS Privacy finds that the Pipeline Operator Security Information collection is privacy sensitive as it collects PII from members of the public (to include U.S. citizens or lawful permanent residents and Non-U.S. Persons).</p> <p>This collection includes voluntary reporting of suspicious activities or security incident data by pipeline industry representatives to TSA’s Transportation Security Operations Center (TSOC) as prescribed in TSA’s Pipeline Security Guidelines available at https://www.tsa.gov/for-industry/surface-transportation. The TSOC will collect the name and contact information (company, phone number, email address) of the reporter. Individuals call or email the TSOC to submit their inquiries. TSA requests that the following also be included in incident reporting: • The time and location of the incident, as specifically as possible; • A description of the incident or activity involved; • Which entities have been notified and what actions have been taken; • The names and/or descriptions of persons involved or suspicious parties and license plates as appropriate. The collection of the incident information is covered by DHS/TSA/PIA-029 Operations Center Incident Management System. Incident reports can be retrieved by Incident number; location; “pipeline.”</p> <p>PRIV agrees with TSA Privacy that PIA coverage is provided under DHS/ALL/PIA-006 DHS General Contacts and DHS/TSA/PIA-029 Operations Center Incident Management System (for incidents). DHS/ALL/PIA-006 outlines how DHS collects contact information in order to distribute information and perform various other administrative tasks. DHS/TSA/PIA-029 outlines how the Transportation Security</p>	



Operations Center TSOC uses WebEOC to perform incident management, coordination, and situational awareness functions for all modes of transportation.

SORN coverage for incident reporting and the collection/retrieving of available PII therein is provided by DHS/TSA-001 Transportation Security Enforcement Record System and DHS/TSA-011 Transportation Security Intelligence Service Files.

DHS/TSA-001 outlines how TSA maintains an enforcement and inspections system for all modes of transportation for which TSA has security related duties and to maintain records related to the investigation or prosecution of violations or potential violations of Federal, State, local, or international criminal law. DHS/TSA-011 outlines how TSA maintain records on intelligence, counterintelligence, transportation security, and information systems security matters as they relate to TSA's mission of protecting the nation's transportation systems. To identify potential threats to transportation security, uphold and enforce the law, and ensure public safety.

A Privacy Act Statement is not required as information is not retrieved via personal identifier. Records are retrieved by incident number; location; pipeline.