



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:	Click here to enter text.		
Form Title:	Click here to enter text.		
Component:	Transportation Security Administration (TSA)	Office:	OIA

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	TSA Pre-Check Application Program		
OMB Control Number:	1652-0059	OMB Expiration Date:	November 30, 2017
Collection status:	Extension	Date of last PTA (if applicable):	Click here to enter a date.

PROJECT OR PROGRAM MANAGER

Name:	Donald Lombardo		
Office:	OIA/PMD	Title:	Branch Manager, Surface Programs
Phone:	15712271735	Email:	Donald.Lombardo@tsa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Nathan Tsoi		
Office:	OIA/PMD	Title:	Program Analyst



Phone: 15712273225 Email: Nathan.Tsoi@tsa.dhs.gov

SPECIFIC IC/Forms PTA QUESTIONS

1. Purpose of the Information Collection or Form

- a. Describe the purpose of the information collection or form. *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).*
If this is an updated PTA, please specifically describe what changes or upgrades are triggering the update to this PTA.

The TSA Pre✓[®] Application Program is a voluntary passenger prescreening initiative for low-risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints. The TSA Pre✓[®] Application Program enhances aviation security by permitting TSA to better focus its limited security resources on passengers who are more likely to pose a threat to civil aviation, while also facilitating and improving the commercial aviation travel experience for the public.

TSA uses the information provided by applicants to conduct security threat assessments (STAs) of the applicants and to conduct screening at airport checkpoints.

- b. List the DHS (or component) authorities to collect, store, and use this information. *If this information will be stored and used by a specific DHS component, list the component-specific authorities.*

Section 109(a)(3) of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (Nov. 19, 2001, codified at 49 U.S.C. § 114 note) provides TSA with the authority to “establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.” In addition, TSA has statutory authority to establish and collect a fee for any registered traveler program by publication of a notice in the Federal Register, as outlined in the Department of Homeland Security Appropriations Act, 2006, Pub. L. 109-90 (Oct. 18, 2005).



2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information” (PII ¹)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
b. From which type(s) of individuals does this form collect information? (Check all that apply.)	<input checked="" type="checkbox"/> Members of the public <ul style="list-style-type: none"> <input checked="" type="checkbox"/> U.S. citizens or lawful permanent residents <input type="checkbox"/> Non-U.S. Persons. <input type="checkbox"/> DHS Employees <input type="checkbox"/> DHS Contractors <input type="checkbox"/> Other federal employees or contractors.
c. Who will complete and submit this form? (Check all that apply.)	<input checked="" type="checkbox"/> The record subject of the form (e.g., the individual applicant). <input type="checkbox"/> Legal Representative (preparer, attorney, etc.). <input type="checkbox"/> Business entity. If a business entity, is the only information collected business contact information? <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Law enforcement. <input type="checkbox"/> DHS employee or contractor. <input type="checkbox"/> Other individual/entity/organization that is NOT the record subject. <i>Please describe.</i> Click here to enter text.
d. How do individuals complete the form? Check all that apply.	<input type="checkbox"/> Paper. <input checked="" type="checkbox"/> Electronic. (ex: fillable PDF) <input checked="" type="checkbox"/> Online web form. (available and submitted via the internet) Provide link: https://universalenroll.dhs.gov

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.



e. What information will DHS collect on the form? *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.*

Name (including aliases or variations of spelling).
Gender.
Current and historical contact information (including, but not limited to, address information, telephone number, and email).
Preferred language
Preferred method of contact
Government-issued licensing or identification information (including, but not limited to, Social Security Number [optional]);
Employment information and occupation
Criminal history record
Date and place of birth
Country of citizenship
Physical description
Other biometric identifier (fingerprint, iris, and/or photograph)

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

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

Section 109(a)(3) of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (Nov. 19, 2001, codified at 49 U.S.C. § 114 note) provides TSA with the authority to “establish requirements to implement trusted passenger programs and use available technologies to expedite security screening of passengers who participate in such



programs, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.” SSN is not mandatory, but is helpful to conduct the security threat assessment.

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.

Collection of SPII is used to conduct a Security Threat Assessment prior to TSA determining an individual applicant’s eligibility to receive expedited screening at airport checkpoints. It will also be used in the airport screening process.

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.
Notice is provided on the form or during the online enrollment process.
- No.

3. How will DHS store the IC/form responses?

a. How will DHS store the original, completed IC/forms?

- Paper. Please describe.
[Click here to enter text.](#)
- Electronic. Please describe the IT system that will store the data from the form.
The Screening Gateway system.
- 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

- Manually (data elements manually entered). Please describe.



<p>responses into the IT system?</p>	<p>Click here to enter text.</p> <p><input checked="" type="checkbox"/> Automatically. Please describe.</p> <p>The Screening Gateway system captures applicant information in XML batches from TSA’s enrollment contractor.</p>
<p>c. How would a user search the information submitted on the forms, <i>i.e.</i>, how is the information retrieved?</p>	<p><input checked="" 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.</p> <p>Information can be retrieved via name, SSN, and/or a Known Traveler Number generated by TSA’s contractor upon an applicant’s enrollment.</p> <p><input type="checkbox"/> By a non-personal identifier. <i>Please describe.</i></p> <p>Click here to enter text.</p>
<p>d. What is the records retention schedule(s)? <i>Include the records schedule number.</i></p>	<p>N1-560-06-6: TSA will retain the data it receives in accordance with record schedules approved by the National Archives and Records Administration (NARA). TSA will retain records for individuals who are not a match or potential match to a watchlist for one year after the individual no longer has TSA Pre✓® eligibility. In addition, for those individuals who may originally have appeared to be a match to a watch list, but subsequently cleared, TSA will retain the records for at least seven years, or one year after TSA Pre✓® eligibility has been terminated, whichever is later. For individuals who are an actual match to a watch list or otherwise determined to pose a threat to transportation security, TSA will retain the records for 99 years, or seven years after TSA learns that an individual is deceased, whichever is earlier.</p>
<p>e. How do you ensure that records are disposed of or deleted in accordance with</p>	<p>We have automated the Screening Gateway and any associated systems with the above rules.</p>

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.



the retention schedule?	
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>	
<input checked="" type="checkbox"/> Yes, information is shared with other DHS components or offices. Please describe. We expect to enroll individuals in DHS OBIM IDENT in November 2017. <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. Fingerprints and associated PII are shared with the FBI to perform a criminal history records check. <input type="checkbox"/> No. Information on this form is not shared outside of the collecting office.	



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:	Peter Pietra
Date submitted to component Privacy Office:	July 7, 2017
Date submitted to DHS Privacy Office:	July 18, 2017
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 checked="" type="checkbox"/> Yes. Please include it with this PTA submission. <input type="checkbox"/> No. Please describe why not. Click here to enter text.
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>	
Privacy Act Statement is attached. PIA coverage is under DHS/TSA/PIA-041 TSA Precheck Application Program. TSA will submit a PIA update or stand-alone PIA if biometrics are ever used to verify identity at the checkpoint. SORN coverage is DHS/TSA-21 TSA Precheck Application Program.	



PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	Sean McGuinness
PCTS Workflow Number:	1148677
Date approved by DHS Privacy Office:	August 16, 2017
PTA Expiration Date	August 16, 2020

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 checked="" 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. Privacy Act Statement approved concurrently with this PTA
PTA:	No system PTA required. Click here to enter text.
PIA:	System covered by existing PIA



	<p>If covered by existing PIA, please list: DHS/TSA/PIA-041 TSA Precheck Application Program If a PIA update is required, please list: Click here to enter text.</p>
<p>SORN:</p>	<p>System covered by existing SORN If covered by existing SORN, please list: DHS/TSA-021 TSA Precheck Application Program, September 10, 2013, 78 FR 55274 If a SORN update is required, please list: Click here to enter text.</p>
<p>DHS Privacy Office Comments: <i>Please describe rationale for privacy compliance determination above.</i></p>	
<p>DHS Privacy Office finds that the TSA Pre-Check Application Program is privacy sensitive as it collects PII from members of the public (U.S. Citizens or lawful permanent residents).</p> <p>The TSA Pre✓® Application Program is a voluntary passenger prescreening initiative for low-risk passengers who are eligible to receive expedited screening at participating U.S. airport security checkpoints.</p> <p>PRIV agrees with TSA Privacy that PIA coverage is provided under DHS/TSA/PIA-041 TSA Precheck Application Program. DHS/TSA/PIA-041 outlines the TSA Pre✓® Application Program and how TSA performs security threat assessments (STA) on individuals who seek eligibility for expedited screening at participating U.S. airport security checkpoints. TSA states that they will submit a PIA update or stand-alone PIA if biometrics are ever used to verify identity at a checkpoint.</p> <p>PRIV agrees with TSA Privacy that SORN coverage is provided under DHS/TSA-021 TSA Precheck Application Program. DHS/TSA-021 outlines how TSA collects and maintains records on individuals who voluntarily submit information to the TSA for use by the agency to perform a STA. The STA will be used to identify persons who pose a low risk to transportation security and therefore may be eligible for expedited screening at participating U.S. airport security checkpoints.</p> <p>A Privacy Act Statement is required as this form collects PII via personal identifier. The Privacy Act Statement is being approved concurrently with this PTA.</p>	