Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

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 Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

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:	TSA Form 2802		
Form Title:	Security Appointment Center (SAC) Visitor Request Form and Foreign National Vetting Request		
Component:	Transportation Security Administration (TSA)	**Office:**	Physical Security, Security Management Section, Security Services and Assessment Division (SSA), Office of Law Enforcement/Federal Air Marshal Service

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	Security Appointment Center (SAC) Visitor Request Form and Foreign National Vetting Request		
OMB Control Number:	1652-NEW	**OMB Expiration Date:**	New
Collection status:	New Collection	**Date of last PTA (if applicable):**	New

PROJECT OR PROGRAM MANAGER

Name:	Larry Carbone

Office:	Physical Security, SSA, OLE/FAMS	**Title:**	Chief , Physical Security
Phone:	571-227-4344	**Email:**	larry.carbone@tsa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:	Jessy Saini		
Office:	OCS, Policy, OLE/FAMS	Title:	Program Analyst
Phone:	703-487-0045	Email:	jessy.k.saini@ole.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.

TSA has established a visitor management/vetting process that meets DHS requirements. This process allows TSA to conduct business with visitors and guest workers, while managing risks posed by individuals entering the building who have not been subject to a full employee security background check. Once vetted, TSA's Visitor Management System (VMS) generates temporary paper badges with photographs that visitors must wear when entering TSA facilities in the National Capital Region (NCR) for the duration of their visit. Under TSA's current visitor management/vetting process, visitors seeking to enter the TSA facilities must request access in person or through a current TSA employee by completing TSA Form 2802, Security Appointment Center (SAC) Visitor Request Form. TSA Form 2802 requires that visitors provide their first and last name, date and time of visit, visitor type (DHS or other government visitor), and whether they are a foreign or national visitor. In order to complete the new vetting process, TSA must collect Personally Identifiable Information (PII). The information collection includes the information TSA previously collected, and date of birth and social security number. TSA will use this information to vet visitors via the NCIC Wants & Warrants/Criminal History Checks and maintain records of access to TSA facilities.

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.***

The Secretary of the Department of Homeland Security (DHS) is authorized to protect property owned, occupied, or secured by the Federal Government. See 40 U.S.C. 1315. See also 41 CFR § 102-81.15 (requires Federal agencies to be responsible for maintaining

security at their own or leased facilities); and EO 9397. DHS Instruction Manual 121-01-011-01 (Visitor Management for DHS Headquarters and DHS Component Headquarters Facilities (April 19, 2014)) requires all DHS components to vet visitors using the National Crime Information Center (NCIC) Wants & Warrants/Criminal History checks before allowing them access to the building.

2. Describe the IC/Form	
a. Does this form collect any Personally Identifiable Information" (PII[1])?	☒ Yes ☐ No
b. From which type(s) of individuals does this form collect information? (*Check all that apply*.)	☒ Members of the public ☒ U.S. citizens or lawful permanent residents ☒ Non-U.S. Persons. ☐ DHS Employees ☐ DHS Contractors ☐ Other federal employees or contractors.
c. Who will complete and submit this form? (*Check all that apply*.)	☐ The record subject of the form (e.g., the individual applicant). ☐ Legal Representative (preparer, attorney, etc.). ☐ Business entity. If a business entity, is the only information collected business contact information? ☐ Yes ☐ No ☐ Law enforcement. ☒ DHS employee or contractor. ☐ Other individual/entity/organization **that is NOT the record subject**. *Please describe*. Click here to enter text.

[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.

d. **How do individuals complete the form?** ***Check all that apply.***	☐ Paper. ☒ Electronic. (ex: fillable PDF) ☐ Online web form. (available and submitted via the internet) *Provide link:*

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.***

TSA Form 2802 requires that visitors provide their first and last name, date and time of visit, visitor type (DHS or other government visitor), and whether they are a foreign or national visitor. TSA must collect Personally Identifiable Information (PII). The information collection includes the information TSA previously collected, and date of birth and social security number. TSA must collect PII such as date of birth, and a passport number from Foreign National Visitors.

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.*

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

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

The Secretary of the Department of Homeland Security (DHS) is authorized to protect property owned, occupied, or secured by the Federal Government. See 40 U.S.C. 1315. See also 41 CFR § 102-81.15 (requires Federal agencies to be responsible for maintaining security at their own or leased facilities); and EO 9397.

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.	
The collection of PII is the minimum amount of information that can properly vet visitors while managing risks posed by individuals entering the building who have not been subject to a full employee security background check.	
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. **Sponsors are directed to provide the following notice to visitors at the time of collection:** AUTHORITY: 40 U.S.C. § 1315; 41 C.F.R. Part 102-81; E.O. 9397. PURPOSE: The information will be used to conduct screening checks to permit and maintain records of access to DHS facilities. ROUTINE USES: The information requested on this form may be shared externally as a "routine use" to the Department of Justice Federal Bureau of Investigation and other government agencies as part of the screening process. A complete list of the routine uses can be found in the system of records notice, "Department of Homeland Security/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records." CONSEQUENCES OF FAILURE TO PROVIDE INFORMATION: Providing this information, including SSN, is voluntary. However, failure to provide the information requested may result in being denied access to a DHS facility; failure to provide the SSN may prevent completion of screening. ☐ 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 online visitor request form is stored on a secured section of iShare, TSA's Intranet.** ☐ 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?	☐ Manually (data elements manually entered). Please describe. Click here to enter text. ☒ Automatically. Please describe. **Once a visitor request is processed, the form is automatically stored on the secured section of iShare, TSA's Intranet.**
c. How would a user search the information submitted on the forms, *i.e.*, how is the information retrieved?	☒ By a unique identifier.[2] *Please describe*. If information is retrieved by personal identifier, please submit a Privacy Act Statement with this PTA. **Each user has his/her own Sponsor Dashboard on iShare, where any and all requests he/she has submitted are available to append. The user is the only individual who can view his/her requests.** ☐ By a non-personal identifier. *Please describe*. Click here to enter text.
d. What is the records retention schedule(s)?	**The records are maintained on the secured iShare section for 2 years, as per NARA requirements, under Schedule 18.**

[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.

Include the records schedule number.	
e. **How do you ensure that records are disposed of or deleted in accordance with the retention schedule?**	**The information technology specialist assigned will ensure that electronic records older than 2 years are permanently destroyed.**
f. Is any of this information shared outside of the original program/office? *If yes, describe where (other offices or DHS components or external entities) and why. What are the authorities of the receiving party?*	
☐ Yes, information is shared with other DHS components or offices. Please describe. Click here to enter text. ☐ Yes, information is shared *external* to DHS with other federal agencies, state/local partners, international partners, or non-governmental entities. Please describe. Click here to enter text. ☒ No. Information on this form is not shared outside of the collecting office.	

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

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD REVIEW

(TO BE COMPLETED BY COMPONENT PRIVACY OFFICE)

Component Privacy Office Reviewer:	**Jennifer L. Schmidt**
Date submitted to component Privacy Office:	**March 7, 2017**
Date submitted to DHS Privacy Office:	March 7, 2017
Have you approved a Privacy Act Statement for this form? (*Only applicable if you have received a waiver from the DHS Chief Privacy Officer to approve component Privacy Act Statements.*)	☒ Yes. Please include it with this PTA submission. ☐ No. Please describe why not. Click here to enter text.
Component Privacy Office Recommendation: *Please include recommendation below, including what existing privacy compliance documentation is available or new privacy compliance documentation is needed.*	
Covered by existing DHS/TSA/PIA-004, Visitor Management System updated 01/06/2017 and DHS/ALL-024, DHS Facility and Perimeter Access Control and Visitor Management published 02/03/2010, 75 FR 5609. **TSA Privacy Office recommends approval.**	

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
202-343-1717, pia@hq.dhs.gov
www.dhs.gov/privacy

PRIVACY THRESHOLD ADJUDICATION

(TO BE COMPLETED BY THE DHS PRIVACY OFFICE)

DHS Privacy Office Reviewer:	**Sean McGuinness**
PCTS Workflow Number:	**1140523**
Date approved by DHS Privacy Office:	March 21, 2017
PTA Expiration Date	March 21, 2020

DESIGNATION

Privacy Sensitive IC or Form:	**Yes If "no" PTA adjudication is complete.**
Determination:	☐ PTA sufficient at this time. ☐ Privacy compliance documentation determination in progress. ☐ New information sharing arrangement is required. ☐ DHS Policy for Computer-Readable Extracts Containing SPII applies. ☒ Privacy Act Statement required. ☒ Privacy Impact Assessment (PIA) required. ☒ System of Records Notice (SORN) required. ☐ Specialized training required. ☐ 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:	**New e(3) statement is required.** Privacy Act Statement approved concurrently with this PTA.
PTA:	**No system PTA required.** Click here to enter text.
PIA:	**System covered by existing PIA**

	If covered by existing PIA, please list: DHS/TSA/PIA-004, Visitor Management System If a PIA update is required, please list: Click here to enter text.
SORN:	**System covered by existing SORN** If covered by existing SORN, please list: DHS/ALL-024, DHS Facility and Perimeter Access Control and Visitor Management If a SORN update is required, please list: Click here to enter text.
DHS Privacy Office Comments: *Please describe rationale for privacy compliance determination above.*	

DHS Privacy Office finds that the Security Appointment Center (SAC) Visitor Request Form and Foreign National Vetting Request is privacy sensitive as it collects PII from members of the public including U.S. citizens or lawful permanent residents and Non-U.S. Persons.

This form collects PII in order to clear visitors that are attempting to gain access to TSA facilities. Therefore allowing TSA to conduct business with visitors and guest workers, while managing risks posed by individuals entering the building who have not been subject to a full employee security background check. Once vetted, TSA's Visitor Management System (VMS) generates temporary paper badges with photographs that visitors must wear when entering TSA facilities in the National Capital Region (NCR) for the duration of their visit.

PRIV agrees with TSA Privacy that PIA coverage is provided under DHS/TSA/PIA-004, Visitor Management System. DHS/TSA/PIA-004 outlines the TSA security requirements and procedures used to manage visitors entering TSA facilities.

PRIV agrees with TSA Privacy that SORN coverage is provided under DHS/ALL-024, DHS Facility and Perimeter Access Control and Visitor Management. The purpose of this system is to collect and maintain records related to DHS facility and perimeter access control, including access to DHS information technology and access to classified facilities, as well as visitor security and management.

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.