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:	**N/A**		
Form Title:	**N/A**		
Component:	Transportation Security Administration (TSA)	Office:	Policy, Plans & Engagement (PPE)

IF COVERED BY THE PAPERWORK REDUCTION ACT:

Collection Title:	**Airport Operator Security**		
OMB Control Number:	1652-0003	OMB Expiration Date:	April 30, 2024
Collection status:	Extension	Date of last PTA (if applicable):	July 19, 2023

PROJECT OR PROGRAM MANAGER

Name:	**Chris Millott**		
Office:	PPE	Title:	Program Manager
Phone:	**317 464 7020**	Email:	Christopher.millott@tsa.dhs.gov

COMPONENT INFORMATION COLLECTION/FORMS CONTACT

Name:Nicole Raymond			
Office:	IT	Title:	PRA Officer
Phone:	703-507-0442	Email:	Nicole.raymond@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 regulations require aircraft operators operating under a full security program, a private charter program, or a full all-cargo program to perform fingerprint-based criminal history records checks (CHRCs) on individuals with unescorted access to secured areas of airports, individuals authorized to perform screening functions, and individuals to perform checked baggage or cargo functions; to maintain records of compliance with this and other requirements; and to provide these compliance records to TSA or make them available for inspection by TSA. TSA's Transportation Security Inspectors (TSIs) coordinate inspections with the aircraft operator's designated Aircraft Operator Security Coordinator (AOSC).

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.*

49 USC 44936; 49 CFR parts 1544.229 through 230.

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/Contractors (list Components) ☐ 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/contractor. ☐ Other individual/entity/organization **that is NOT the record subject**. *Please describe*. Click here to enter text.
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:*

[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 individual 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 collects the AOSC's business contact information (company name, address, phone number and email address) including a phone number that the AOSC can be reached at 24/7.

To comply with TSA regs, aircraft operators must collect the following from employees who require unescorted access to secure areas of the airport for purposes of vetting: Full name and any aliases; gender; DOB; POB; SSN; home address, phone number, submitting entity (employer or prospective employer); fingerprints along with race, height, weight, eye color, and hair color; citizenship, and if applicable, passport number and country of issuance; ARN or certificate of naturalization or birth abroad.

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
☒ Alien Number (A-Number)
☐ Tax Identification Number
☐ Visa Number
☒ Passport Number
☐ Bank Account, Credit Card, or other financial account number
☐ Other. *Please list:*

☐ DHS Electronic Data Interchange Personal Identifier (EDIPI)
☐ Social Media Handle/ID
☐ Known Traveler Number
☐ Trusted Traveler Number (Global Entry, Pre-Check, etc.)
☐ Driver's License Number
☒ Biometrics

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

EO 9397; 49 USC 44936; 49 CFR parts 1544.229 through 230.

h. How will the SSN and SPII information be used? What is the purpose of the collection?

This information is used to ensure security threat assessments are being conducted on airport employees needing unescorted access to secure areas.

i. Is SSN necessary to carry out the functions of this form and/or fulfill requirements of the information collection? *Note*: even if you are properly authorized to collect SSNs, you are required to use an alternative identifier. If there are technological, legal, or regulatory limitations to eliminating the SSN, privacy-enhancing alternatives should be taken, such as truncating the SSN.	
Yes	
j. 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. Aircraft operators are required to make available to applicants and employees the Privacy Act statement when they submit for an initial or renewal CHRC. ☐ 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. Click here to enter text. ☐ 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. Click here to enter text.

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. In rare circumstances, when an incident involves an egregious violation by an aircraft operator employee (and not an incident of general non-compliance on the operator's behalf) inspection records may be categorized and retrieved by the individual's name. ☐ By a non-personal identifier. *Please describe*. Click here to enter text.
d. What is the records retention schedule(s)? *Include the records schedule number.*	TSA Disposition schedule 400.19.1: Includes, but not limited to, security-related incidents, reports, profiles, subject history, inspections, investigative data, security threat assessments (STA), workbooks, dashboards and other records used to support agency programs by documenting and tracking actions to either complete or support findings of inspections, investigations, security threat assessments, legal proceedings (criminal or civil) and enforcements. Cut off annually in year in which case is closed. Destroy 7 years after cutoff in accordance with NARA authority, N1-560-12-002 item 3.
e. How do you ensure that records are disposed of or deleted in accordance with the retention schedule?	The office of Security Operations (SO) records liaison reviews records annually for records that may be deleted.
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.	

[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.

☐ 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:	**William Feeney**
Date submitted to Component Privacy Office:	**June 4, 2024**
Concurrence from other Components involved (if applicable):	Click here to enter text.
Date submitted to DHS Privacy Office:	June 4, 2024
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.

PIA coverage provided by DHS/TSA/PIA-020, Security Threat Assessments for Airport Badge and Credential Holders (SIDA). SORN coverage is provided by DHS/TSA/SORN-002, Transportation Security Threat Assessment System. TSA Privacy recommends no further privacy documentation.

Privacy Act Statement:
Authority: 6 U.S.C. § 1140, 46 U.S.C. § 70105; 49 U.S.C. §§ 106, 114, 5103a, 40103(b)(3), 40113, 44903, 44935-44936, 44939, and 46105; the Implementing Recommendations of the 9/11 Commission Act of 2007, § 1520 (121 Stat. 444, Public Law 110-53, August 3, 2007); FAA Reauthorization Act of 2018, §1934(c) (132 Stat. 3186, Public Law 115-254, Oct 5, 2018), and Executive Order 9397, as amended.

Purpose: The Department of Homeland Security (DHS) will use the biographic information to conduct a security threat assessment. Your fingerprints and associated information will be provided to the Federal Bureau of Investigation (FBI)

for the purpose of comparing your fingerprints to other fingerprints in the FBI's Next Generation Identification (NGI) system or its successor systems including civil, criminal, and latent fingerprint repositories. The FBI may retain your fingerprints and associated information in NGI after the completion of this application and, while retained, your fingerprints may continue to be compared against other fingerprints submitted to or retained by NGI. DHS will also transmit your fingerprints for enrollment into US-VISIT Automated Biometrics Identification System (IDENT). DHS may provide your name and SSN to the Social Security Administration (SSA) to compare that information against SSA records to ensure the validity of the information.

Routine Uses: In addition to those disclosures generally permitted under 5 U.S.C. 522a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 522a(b)(3) including with third parties during the course of a security threat assessment, employment investigation, or adjudication of a waiver or appeal request to the extent necessary to obtain information pertinent to the assessment, investigation, or adjudication of your application or in accordance with the routine uses identified in the TSA system of records notice (SORN) DHS/TSA 002, Transportation Security Threat Assessment System. For as long as your fingerprints and associated information are retained in NGI, your information may be disclosed pursuant to your consent or without your consent as permitted by the Privacy Act of 1974 and all applicable Routine Uses as may be published at any time in the Federal Register, including the Routine Uses for the NGI system and the FBI's Blanket Routine Uses.

Disclosure: Pursuant to § 1934(c) of the FAA Reauthorization Act of 2018, TSA is required to collect your SSN on applications for Secure Identification Display Area (SIDA) credentials. For SIDA applications, failure to provide this information may result in denial of a credential. For other aviation credentials, although furnishing your SSN is voluntary, if you do not provide the information requested, DHS may be unable to complete your security threat assessment.

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:	**Ke'Angela Crawford**
PCTS Workflow Number:	**0017264**
Date approved by DHS Privacy Office:	June 14, 2024
PTA Expiration Date	June 14, 2027
DHS Privacy Office Approver (if applicable):	**Riley Dean**

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.
Privacy Act Statement:	**e(3) statement update is required.** **A Privacy Act Statement is required as information may be retrieved via unique identifier. In certain circumstances when an incident involves an egregious violation by an aircraft operator employee (and not an incident of general non-compliance on the operator's behalf) inspection records may be categorized and retrieved by the individual's name. Aircraft operators are required to make available to applicants and employees the Privacy Act statement when they submit for an initial or renewal CHRC. Otherwise, inspection records are routinely retrieved by an**

	incident/inspection report tracking number created by PARIS. PRIV recommends adding a line in the Routine Uses section of the Privacy Act Statement that says something along the lines of, "for those individuals not covered by the Privacy Act, please refer to DHS/TSA/PIA-020 Airport Access for Aviation Workers" as this form will potentially collect information from non-U.S. Persons. Privacy Act Statement approved along with this PTA.
System 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-020 Airport Access for Aviation Workers.** 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/TSA-002 Transportation Security Threat Assessment System, August 11, 2014, 79 FR 46862.** 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.

TSA is submitting this renewal PTA for the Airport Operator Security form. There have been no changes since the previously approved PTA.

The Airport Operator Security form enforces TSA regulations by requiring certain aircraft operators to conduct fingerprint-based criminal history checks on specific individuals, maintain compliance records, and provide these records to the TSA for inspection. The forms are submitted to TSA to complete the security threat assessment (STA) and they must also be retained locally for inspections. The specific process depends on the purpose of the STA; it may involve various systems or simply be emailed to TSA. For example, the portal for cargo handlers can be found here https://iac.tsa.dhs.gov/iac/.

The DHS Privacy Office (PRIV) concurs that this is a privacy-sensitive form because it collects PII and SPII from members of the public. PRIV recommends coverage under DHS/TSA/PIA-020 Airport Access for Aviation Workers, which describes how TSA conducts STA on individuals seeking or holding authorized airport badges or credentials and the requirement to conduct fingerprint-based criminal history

record checks (CHRCs) along with name-based checks on individuals requiring unescorted access to the sterile area of the airport.

Data can be retrieved by a unique identifier, therefore, SORN coverage is required. SORN coverage is provided under DHS/TSA-002 Transportation Security Threat Assessment System, which covers how TSA collects and maintains records related to STA, employment investigations, and evaluations that the TSA conducts on certain individuals for security purposes.

A Privacy Act Statement is required as information may be retrieved via unique identifier. In certain circumstances when an incident involves an egregious violation by an aircraft operator employee (and not an incident of general non-compliance on the operator's behalf) inspection records may be categorized and retrieved by the individual's name. Aircraft operators are required to make available to applicants and employees the Privacy Act statement when they submit for an initial or renewal CHRC. Otherwise, inspection records are routinely retrieved by an incident/inspection report tracking number created by PARIS. PRIV recommends adding a line in the Routine Uses section of the Privacy Act Statement that says something along the lines of, "for those individuals not covered by the Privacy Act, please refer to DHS/TSA/PIA-020 Airport Access for Aviation Workers" as this form will potentially collect information from non-U.S. Persons. Privacy Act Statement approved along with this PTA.