

TRIP PIA**1. Contact Information**

A/GIS/IPS Director Bureau of Administration Global Information Services Office of Information Programs and Services

2. System Information

(a) **Name of system:** Tracking Responses and Inquiries for Passports

(b) **Bureau:** Bureau of Consular Affairs (CA)

(c) **System acronym:** TRIP

(d) **iMatrix Asset ID Number:** 2677

(e) **Reason for performing PIA:**

- New system
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

(f) **Explanation of modification (if applicable):**

3. General Information

(a) **Does the system have a completed and submitted Security Categorization Form (SCF)?**

- Yes
- No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) **What is the security assessment and authorization (A&A) status of the system?**

TRIP received a one year Authorization To Operate in January 2015. Another assessment and authorization of this system is underway and is expected to be completed by January 2016. This document was updated as part of that reauthorization of the system.

(c) Describe the purpose of the system:

TRIP supports the Bureau of Consular Affairs mission requirements to allow CA to keep records of every contact and transaction with customers who call the National Passport Information Center (NPIC) to inquire about the status of their passport application. A transaction is typically a notification sent by NPIC to a passport agency requesting that the agency contact a customer directly to discuss specifics of a passport application in process.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

TRIP collects the following information: name, home phone number, address, date of birth (DOB), Social Security number (SSN), and, when a customer is requesting to upgrade his/her application to expedited processing, credit card number.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1104 (Powers and Duties of Secretary of State)
- 8 U.S.C. 1401–1503 (Acquisition and Loss of U.S. Citizenship or U.S. Nationality)
- 18 U.S.C. 911, 1001, 1541–1545 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705
- Executive Order 11295 (August 5, 1966)
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Control of Citizens)
- 22 CFR Parts 50 and 51

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes

If yes, provide:

- **SORN Name and Number:** Passport Records, STATE-26
- **SORN publication date:** March 24, 2015

No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

Yes

No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

Yes

No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide:

Schedule number (e.g., (XX-587-XX-XXX)):

Length of time the information is retained in the system:

Type of information retained in the system:

While there isn't a specific records retention schedule for this system, there are records retention schedules regarding passport records. The one most applicable to this system would be Chapter 13 Passport Records, Section 001.

A-13-001-23 Routine Passport Application Status Check and Expedite Fee Upgrades E-mail.

Description: E-mail messages regarding the status of passport applications and requests for expedited service.

Disposition: TEMPORARY: Destroy/delete when 25 days old.

DispAuthNo: N1-059-98-3, item 1

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

Members of the Public

- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

- Yes
- No

If yes, under what authorization?

[26 U.S.C. 6039E](#) – Information Concerning Resident Status

(c) How is the information collected?

The information in TRIP is collected by telephone when the applicant calls NPIC and speaks to a Customer Service Representative (CSR).

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?

The information requested of inquirers is confirmed against the information on the passport or passport application contained in Travel Document Issuance System (TDIS). Accuracy of the information contained in TDIS (such as a passport application or submission of citizenship evidence) is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

If the applicant’s application appears in TRIP (which mirrors information in TDIS) and any of the information is incorrect (when the CSR verifies it with the passport applicant) then the CSR will request the correct information from the passport applicant and will send a notification email to the adjudicating passport agency requesting an update to the applicant’s information in TDIS.

(g) Does the system use information from commercial sources? Is the information publicly available?

TRIP does not use any commercial information.

(h) Is notice provided to the individual prior to the collection of his or her information?

Individuals are made aware of the uses of the information prior to collection, at the beginning of the phone call.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

Yes

No

If yes, how do individuals grant consent?

They are advised that they can decline to provide the information requested. However, in that case, they cannot receive information on the status of their passport application through TRIP.

If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The information collected is necessary for the processing of passport applications and in responding to application status inquiries by the applicant. The PII is handled in accordance with federal privacy regulations regarding the collection, access, disclosure, and storage of PII. TRIP is designed so that neither SSNs nor credit card numbers are maintained beyond the length of a call.

5. Use of information

(a) What is/are the intended use(s) for the information?

The TRIP system allows CA/CST and CA/PPT to keep records on every contact with applicants who call NPIC to inquire about their passport application status. TRIP allows CSRs to bring up TDIS inquiries on passport application records and view the information by searching by the applicant's passport application number, SSN or the

applicant's last name and DOB. The CSR then confirms the identity of the inquirer by requesting the inquirer's PII indicated in Section 3(a) above to ensure that it matches the information in the record. Once the information is confirmed, the CSR may then share the information in the record with the inquirer. Each CSR is able to see a case history as well as generate emails to the passport agency on each applicant if needed. Emails can be generated for each of the 29 Passport Agencies with counters. TRIP also enables each CSR user to access the knowledge base, which contains Department of State travel information that is referenced to help answer customer questions. The applicant's SSN is not maintained in the TRIP database beyond the length of a call. The applicant's passport application number, SSN or the applicant's last name and DOB must be given to the CSR each time the applicant calls to inquire about his/her passport application.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

- Yes
 No

(c) Does the system analyze the information stored in it?

- Yes
 No

If yes:

(1) What types of methods are used to analyze the information?

A CSR enters the applicant's information (the applicant's passport application number, SSN or the applicant's last name and DOB) into TRIP in order to search the TDIS database. The initial step is to query the TDIS system and use the search results to verify if the applicant is already in the TDIS system. If the applicant's passport information already exists in TDIS, then the existing record will be used to relay a passport status to the applicant online or via phone. Upon verification by CSR that the TDIS response pertains to the caller, TRIP transfers the applicant's information into the CSR's call record in a read-only process. The CSRs cannot create new information directly in TDIS (changes or clarification to full names, address, phone numbers, incorrect recording of SSN, DOB, etc.) but can request the changes be made by persons with access to TDIS by typing the call notes in an email from within TRIP (which automatically retrieves applicant information from within the system) that is sent to the adjudicating agency either requesting additional information or relaying new information.

(2) Does the analysis result in new information?

It may if inaccuracies are discovered.

(3) Will the new information be placed in the individual's record? Yes No**(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?** Yes No**6. Sharing of Information****(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.**

Internal: Information is shared between TRIP and TDIS by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

TRIP does not share information externally.

(b) What information will be shared?

Social Security number (SSN), passport application number, the applicant's last name and date of birth.

(c) What is the purpose for sharing the information?

The information obtained by TRIP CSRs is used for the purpose of retrieving TDIS records through TRIP to respond to passport applicants' inquiries regarding the status of their applications.

(d) The information to be shared is transmitted or disclosed by what methods?

Information is shared between TRIP and TDIS by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

(e) What safeguards are in place for each internal or external sharing arrangement?

The internal users, system administrators, and database administrators are trained through the security awareness training to safeguard sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that is SBU.

**(f) What privacy concerns were identified regarding the sharing of the information?
How were these concerns addressed?**

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of personal information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure, including but not limited to annual security training, separation of duties, least privilege, personnel screening, and auditing.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The system contains Privacy Act-covered records; therefore, notification and redress are the right of record subjects. Procedures for notification and redress are published in the System of Records Notice (SORN) Passport Records (STATE-26), and in the regulations at 22 CFR 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes

No

If yes, explain the procedures.

The applicant must call the National Passport Information Center (NPIC).

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Individuals who wish to have their records amended can find instructions, submission requirements, and the mailing address in the regulations at 22 CFR 171 and on the Department of State's FOIA website at foia.state.gov/request/guide.aspx.

8. Security Controls

(a) How is the information in the system secured?

The TRIP system is secured within the Department of State intranet where risk factors are mitigated through the use of multiple layers of security controls, including management security, auditing, firewalls, and physical security.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

As a matter of policy, the Department of State Chief Information Officer and Information System Security Officer require certain fundamental procedures for all systems. Potential users are screened and assigned privileges based on their roles, responsibilities and the need-to-know. Specific privileges for a given user are only granted after careful consideration of the user role. There are five types of TRIP user roles: Database Administrator, System/Web Administrator, Contact Center Supervisor, Internal Customer Service Team, and Customer Service Representative. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

The security posture will be considered in terms of operations and administration, audits and monitoring, and operational assurance. Any system modifications are monitored, recorded, and audited to ensure they do not disable or circumvent any established security or assurance controls in place.

(d) Explain the privacy training provided to authorized users of the system.

In accordance with Department of State computer security policies, TRIP users are required to complete the Cyber Security Awareness Training and the PII Training at least once a year. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

- Yes
 No

If yes, please explain.

The information transmitted to the database is encrypted in accordance with Department of State specifications utilizing FIPS 140-2 compliant algorithms. In addition to encrypted transmissions, TRIP leverages Department of State managed Active Directory strong authentication procedures. The information transmitted between workstations and servers is confined to the department's secure internal networks.

(f) How were the security measures above influenced by the type of information collected?

The Department of State has long been concerned with the protection of individuals' personal information in accordance with U.S. government policies. Passport information and the PII contained in passport applications constitute the substantive portion of the information contained in TRIP.

9. Data Access

(a) Who has access to data in the system?

The following personnel have access to the system: Database Administrator, System/Web Administrator, Contact Center Supervisor, Internal Customer Service Team, and Customer Service Representative.

(b) How is access to data in the system determined?

An individual's job function determines what data can be accessed.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

- Yes
 No

CA/CST adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. In addition, there are documented procedures to facilitate the implementation of the policy and the audit and accountability controls.

(d) Will all users have access to all data in the system or will user access be restricted?

Please explain.

Users have access to TRIP based on their roles and job functions. Therefore, access privileges will vary depending on the role of the user. There are five types of TRIP user roles: Database Administrator, System/Web Administrator, Contact Center Supervisor, Internal Customer Service Team, and Customer Service Representative.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Various controls are implemented at the management, operational, and technical levels. Special attention is paid to recording, monitoring, and auditing of user activity.