1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: December 04, 2008

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

(c) System acronym: TRIP

(d) IT Asset Baseline (ITAB) number: 2677

(e) System description (Briefly describe scope, purpose, and major functions):

TRIP is a web-based application that is composed of commercial-off-the-shelf (COTS) software that has been modified to meet functional requirements. TRIP allows CA/CST to keep records of customers that call National Passport Information Center (NPIC) to inquire about their passport application status. TRIP allows personnel to review Travel Document Issuance System (TDIS) inquires on passport application records. Phone representatives are able to see a case history and generate notes on each case. Emails can be generated for each agency and users can access the knowledge base which contains referenced Department of State information.

TRIP is located at NPIC in Dover, New Hampshire. A second host site for contingency and disaster recovery is located in Lansing, Michigan.

TRIP interfaces with the Front End Processor (FEP) system. TRIP uses FEP to query the TDIS application database for information pertaining to an applicant.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): 2/29/2008

3. Characterization of the Information

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

TRIP does not collect or maintain any PII elements. Instead, TRIP interfaces with Travel Document Issuance System (TDIS). CSRs (Customer Service Representatives) with read-only access directly interface with customer personal data within TDIS. TDIS collects and maintains records related to applications for U.S. passports, including the following categories of records:

- Passport books and passport cards, applications for passport books and passport cards, and applications for additional visa pages, amendments, extensions, replacements, and/or renewals of passport books or cards; and
- Records of lost and stolen passports

Sources of the information are U.S. citizens applying for passports, other Department of State computer systems, passport specialists, and fraud prevention managers. The categories of record subjects in TDIS are individuals who:

- Have applied for the issuance, amendment, extension, or renewal of U.S. passport books and passport cards;
- Were issued U.S. passport books or cards, or had passports amended, extended, renewed, limited, or denied; or
- Have corresponded with Consular Affairs concerning various aspects of the issuance or denial of a specific applicant's U.S. passport books or cards.

Any personally identifiable information referenced by TRIP is maintained by TDIS. CSRs access this information and verify it with the customer before giving out any private information regarding their passport application.

b. How is the information collected?

The information is collected by TDIS via several forms: Form DS-11 is used for passport applications from first time applicants; Form DS-82 is for persons applying to replace a passport issued within the past 15 years, who are over the age of 16 when the passport was issued, and who also provide the old passport with the application form; Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. The form may be used to replace an emergency passport with a full validity one; to make a change to the applicant's identifying information (e.g., name change due to marriage or court order); or to correct a printing error in their passport; Form DS-4085 is used to add visa pages to a previously issued and currently valid passport.

The above forms may be completed by the applicant on published paper forms available at many government office locations or may be completed online using web forms at the Department of State's public web site. If web forms are used, the applicant must still print the form and submit it as hardcopy with supporting documents.

c. Why is the information collected and maintained?

TRIP allows CSRs to respond to phone, letter and email inquiries for passport application status from U.S. citizens. The CSRs query TDIS through the TRIP SQL Server database to view customer applications updates.

d. How will the information be checked for accuracy?

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.

A CSR enters the applicant's SSN, application number or name and date of birth to search the TRIP database. CSRs do not have direct access to TDIS but can access TDIS via a TRIP/TDIS interface. If the applicant already exists in TRIP then the existing record will be used. If the applicant can not be located by the TRIP system search of the TDIS system and they have applied for a passport, the applicant's TDIS new application record has not been created in the TDIS system (usually occurs when the applicant seeks a status the same day or week they applied for the passport).

The CSRs only have access to TRIP which interfaces with TDIS. If applicant's passport information is not already in TDIS, then the CSR cannot see the customer's passport application data or status. If, however, the customer's application appears in TDIS and any of the information is incorrect (when the CSR verifies it with the customer) then the CSR will request the correct information from the customer and will send an email to the adjudicating Agency for them to update the customer's application in TDIS. CSRs have no ability to directly update a customer's information.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The following authorities provide for the administration of the program supported by TRIP:

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (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)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Considering the large amount of personally identifiable information collected by TDIS and accessed by TRIP, the security and privacy controls in place are adequate to safeguard applicant privacy. TRIP utilizes numerous management, operational and technical security controls to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling configuration management, boundary and information integrity protection (eg, firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The TRIP system allows CA/CST to keep records on every contact with customers that call. TRIP allows CA personnel to bring up TDIS inquires on Passport Application records and view the information. Each phone representative is able to see a case history as well as generate notes on each case. Emails can be generated for each agency, and TRIP also enables each user to access the knowledge base, which contains DoS information that is referenced.

b. What types of methods are used to analyze the data? What new information may be produced?

A CSR enters the applicant's information 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. The CSRs can create new TDIS information (changes or clarification to full names; address, phone numbers, incorrect recording of ssn, DOB, etc.) by typing the notes of a call with a passport applicant within the TRIP system and create an email from within TRIP (that automatically contains applicant information) that is sent to the adjudicating agency either requesting additional information or relaying new information.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

TRIP does not use any commercial information.

d. Is the system a contractor used and owned system?

TRIP is a DoS system that is developed and maintained by AT&T. The system is hosted at NPIC in Dover, New Hampshire with a disaster recovery site located in Lansing, Michigan.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Contractors involved in the design, development and maintenance of TRIP are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of TDIS hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor owned facilities are annually inspected by Diplomatic Security.

5. Retention

a. How long is information retained?

The retention period of information is consistent with established Department of State Policies and Guidelines as documented in the DoS Disposition Schedule, Chapter 13, Passport Records.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

None. The data retained in the information system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records; and little privacy risk as a result of degradation of data quality in this information system over an extended period of time.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

TRIP is accessible only through the DoS OpenNet. The CSRs use Internet Explorer (IE) browser to access the TRIP web portal located at Dover, NH and Lansing, Michigan. The backend TRIP servers consist of Contact Center servers, IQ servers, Microsoft SQL Database servers and Response servers. The CSRs connect to the Contact Center servers and submit the type of inquiry from the customer into the SQL database. The CSR can access the information from the Travel Document Issuance System (TDIS) at the passport agency through TRIP. TRIP can be accessed by CSRs/management at the Dover and Lansing sites, DoS Liaison at Dover site, PPT HQ, and PPT Agencies.

Access to the TRIP application will be restricted to cleared, authorized Department of State direct hire or contractor personnel via OpenNet. The TRIP application enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

System administrators can access the TRIP application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entities is strictly prohibited.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Internal sharing occurs only with authorized users, who are cleared government employees or contractors with work-related responsibilities specific to the access and use of the information. No other internal disclosures of the information within the Department of State are made.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

TRIP information will not be shared with other agencies for programmatic purposes. Only authorized Department of State CSRs and authorized Passport Agency personnel have access to the data in the system.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

External access to any non-Department entities is strictly prohibited.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

None. TRIP data is not externally shared or disclosed (TRIP data is only communicated with the applicant whose personal information has first been verified using Privacy Act).

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

Passport Records – STATE-26

Overseas Citizens Services – STATE-05

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Individuals are made aware of the uses of the information prior to collection. Notice is also published in the system of record State-number and name of SORN. U.S. citizens who call CSRs are informed to call NPIC regarding the status of their passport application, the information needed and the purpose for giving the information.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes. They are advised that they can decline to provide the information requested, however, in doing so, their passport status will not be able to be tracked by TRIP.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No other special uses of the information are permitted. Users are advised on the use of the information being collected.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

U.S. citizens that call NPIC via the TRIP system for a status of their passport applications are notified either by the automated voice prompt service or NPIC representative that the purpose of the information/data they are required to give is for locating an accurate status on their pending passport. The caller will give the automated system their social security number or application number, last name and date of application in order for the system to locate their pending passport status; and a status is given. If they talk with an NPIC representative they will be asked their social security number or application number, last name and state of residence; and once their pending passport status has been located they will ask to confirm their full name, date of birth, full address (to include state and zip).

NPIC representatives who utilize and have access to TRIP are restricted to cleared, authorized Department of State direct hires or contractor personnel. TRIP enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

None. TRIP can only be accessed via OpenNet by cleared, authorized Department of State direct hire or contractor NPIC personnel. If a change is required for their passport the proper procedures are relayed to the individual.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the TRIP application is restricted to cleared, authorized Department of State direct hire or contractor personnel via OpenNet. The TRIP application enforces the concept of least privilege by ensuring that users are restricted to only those functions which are required to perform their assigned duties. System administrators can access the TRIP application only at the central server location to perform application maintenance tasks, such as installation of patch updates or modification of the system's customized software functionality. External access to any non-Department entities is strictly prohibited.

Personnel accessing TRIP information must be authorized by NPIC management. Authorized personnel require a user ID/password to access TRIP information. User access to TRIP information is based on roles. The regular users (CSRs) will be allowed to create records and append new data to those records via an email from within the TRIP system that is sent to the TDIS adjudicating agency that will relay new information on the passport applicant. The supervisors are allowed to review and make necessary corrections to the passport applicant record in TRIP. All TRIP users have knowledge of the FAM/FAH policies regarding privacy and are required to obtain annual Security Awareness Training.

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

b. What privacy orientation or training for the system is provided authorized users?

All contractors involved with the design, development, and maintenance have had the Privacy Act contract clauses inserted in their contracts and all other regulatory measures have been addressed. Rules of conduct have been established and training given regarding the handling of such information under the Privacy Act of 1974, as amended.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a user performed – or attempted to perform – on an information system.) As a result of these actions, the residual risk is low.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

TRIP is web-based application with approximately 200 XP Professional workstations and 10 Windows 2003 Servers. TRIP is customized Commercial off-the Shelf (COTS) product designed and developed by Customer Relations Management (CRM) software services vendor KANA. It is customized to track DoS customer inquiries regarding the status of their passport application. These are all tested, proven technologies, and they pose no additional privacy risks.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

None.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates TRIP in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls

on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its 36 month authorization to operate expires February 28, 2011.