PRIVACY IMPACT ASSESSMENT

Tracking Responses and Inquiries for Passports

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

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

The system is currently undergoing its Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. TRIP is expected to receive an ATO by Spring 2021.

(c) Describe the purpose of the system:

The Tracking Response and Inquiries for Passports (TRIP) system provides the Bureau of Consular Affairs Customer Service Representatives (CSR) the capability to maintain and access records of every communication and transaction with customers who contact the National Passport Information Center (NPIC) to inquire about the status of their passport application. TRIP allows the CSR to connect through the Front End Processor (FEP) system to the Travel Document Issuance System (TDIS) to view Passport Application records and case histories, and notes associated with the specific case to address inquiries.

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

TRIP contains the following PII on U.S. Citizens: name, birthdate, place of birth, nationality, gender, Social Security number, passport information or other identification number, phone number, personal address and personal email address.

(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 the Secretary of State)
- 22 U.S.C. Sec. 211a-218, 2651a, 2705 (Passport Application and Issuance)
- 22 U.S.C. 3927 (Chief of Mission)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- Executive Order 11295, August 5, 1966; (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)

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

☒Yes, provide SORN

STATE-26, Passport Records, March 24, 2015
STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016

☐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 Office 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

A-13-002-03 Tracking/Issuance System
Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation
Disposition: Permanent: Delete when twenty-five (25) years old.
DispAuthNo: N1-059-05-11, item 3

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)

☐ U.S. Government/Federal employees or Contractor employees

☐ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(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

22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) How is the information collected?

The information in TRIP is collected from the applicant (over the phone) and entered into TRIP by the NPIC Customer Service Representative (CSR).

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

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

Information provided by individuals is confirmed against the information issued on the passport or passport application contained in Travel Document Issuance System (TDIS). Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimized instances of inaccurate data.

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

Currency is determined by the information provided by the caller when checked against the TRIP and TDIS databases. If the information provided by the passport applicant does not mirror the information in the TRIP and TDIS databases, 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?

No, TRIP does not use commercial or publicly available information.

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

A Privacy Act statement is not required for this system. It is not accessible to the public, only to State Department personnel authorized to access and use TRIP. Individuals are verbally briefed on the use of their information at the beginning of the phone call, prior to collection.

The applicant is verbally briefed via phone on the required notice:

1. The purpose for which the information is required.
2. The possible use of the information
3. How the data is protected from unauthorized/ illicit disclosure.
4. The potential consequences if the applicant declines to provide the data (i.e., that they may not be able to receive a status update on their passport.)

(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?

Individual callers have the option to not provide information to the TRIP Customer Service Representative, or to hang up; however, this may result in the caller not being provided the services desired. Consent is provided when the caller provides the required information after they are verbally briefed on the use of the information.

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 PII listed in Question 3d is the minimum necessary to perform the actions required to provide passport inquiry services to U.S. citizens via the TRIP system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and addressed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the TRIP system to perform the function for which it was intended - to provide access to information to address passport questions and inquiries of U.S. Citizens.

5. Use of information

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

The TRIP system PII is required to assist Department of State Customer Service Representatives in their research to address passport questions and status update requests of U.S. Citizens.

(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. The PII is used according to the purpose for which the system was designed: to provide customer services to U.S. Citizens asking for updates on the status of their passport application or other passport related questions.

(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?

Once the CSR enters the caller-provided information into the system, TRIP compares it with what is in the TDIS system.

(2) Does the analysis result in new information?

☒Yes - If the "compare and contrast" indicates discrepancies in TRIP, new information about the discrepancy is created and the applicant is contacted for correction of data.

☐No

(3) Will the new information be placed in the individual's record?

☒Yes – TRIP discrepancy information is recorded for resolution.

☐No

(4) With the new information, will the State Department be able to make new determinations about the individual that would not have been possible without it?

☒Yes – If the discrepancy in the information provided by the caller is not resolved, it could impact the determination of granting the passport.

☐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 Sharing: TRIP is used within the Bureau of Consular Affairs to process passport applications. The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as "Bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the Bureau. With that understanding, information in the TRIP system will be shared internally with the CA system Travel Document Issuance System (TDIS) via the Front End Processer (FEP) system to address and respond to passport questions and inquiries of U. S. Citizens.

Externally: TRIP does not share externally.

(b) What information will be shared?

The information in paragraph 3d is shared.

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

Information is shared to address and respond to passport inquiries from U. S. Citizens.

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

Information is shared database to database between TRIP, FEP and TDIS by Secure Socket Layer (SSL) authentication transmission methods permitted by 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 information in TRIP is only shared internally. TRIP uses Transmission Control Protocol/Internet Protocol (TCP/IP) to assist with its data transport across the network. The TCP/IP protocol suite consists of multiple layers of protocols that help protect the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary.

The information in and processed by TRIP, FEP and TDIS is accessible only to authorized CA users and is subject to stringent access policies, auditing and monitoring. In accordance with U.S. government policies, any federal government employee or contractor with access to personally

identifiable information (PII) must adhere to strict requirements for protection and storage of PII. Department of State personnel are required to comply with these requirements and to complete yearly training regarding cyber security and the protection of PII.

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

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

a. Accidental disclosure of information to unauthorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

b. Deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other.

The above risk areas are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, "sensitive but unclassified", and all higher levels of classification, and signing a user agreement.

- Strict access control based on roles and responsibilities, authorization and need-to-know.

- System authorization and accreditation process along with continuous monitoring (Risk Management Framework). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

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

U.S. citizens can follow instructions for gaining access as stated in SORNs State-26 and State-05. They may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA web site for the privacy policy which includes instructions on how to obtain access by contacting the listed offices by phone or by mail.

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

☒Yes ☐No

If yes, explain the procedures.

U.S. citizens can follow instructions for requesting changes to their information as stated in SORNs State-26 and State-05, or visit the Department of State Privacy Act/FOIA public web site for the privacy policy which includes instructions on how to request changes by contacting the listed offices by phone or by mail.

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

Individuals are notified of the procedures to correct records in TRIP by a variety of methods:

1. During their phone call when contacting the NPIC Customer Service Representatives regarding passport status updates.
2. Information in the published SORNs STATE-26, Passport Records, March 24, 2015 and STATE-05, Overseas Citizens Services Records and Other Overseas Records, September 8, 2016.
3. Being notified by letter or email that a correction is needed.

Each method contains information on how to amend records and who/what office to get in touch with as well as providing contact information.

If no, explain why not.

8. Security Controls

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

The TRIP system is secured through the use of defense in-depth layers of security, including implementation of management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform their official duties.

Access is further protected with additional access controls set at the application/database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system and any violations are reported to senior management.

Applications are configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) standards, including NIST 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program.

(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.

To access the TRIP system, persons must be authorized users of the Department of State's unclassified internal network (OpenNet), which requires a background investigation and an application approved by the supervisor and the local Information System Security Officer (ISSO). Authorized users are issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access required for logon.

Each authorized user must agree to the user access agreement/rules of behavior before being given a user account and accessibility to the TRIP system. Access to the TRIP system is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Local ISSOs determine the access level needed by a user (including managers) to ensure it correlates to the user's approved particular job function and level of clearance.

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

The CA System Manager and CA ISSO, in conjunction with the CA Security team, periodically scan and monitor information systems for compliance with Department of State Diplomatic Security (DS) Configuration Guides and conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the CA systems, including this specific system.

Access control lists on all Department of State servers and devices along with DS Security Configuration Guide standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with DS Security Configuration Guides, auditing is enabled to track the following events on the host operating systems and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training which has a privacy component to access or use the systems. Additionally, Department of State personnel are required to take the biennial course PA318, Protecting Personally Identifiable Information. In addition to the above required training, the Passport Services Internal Control Guide requires all personnel (government and contractors) to complete the Passport Data Security Awareness (PC441) course and pass the course as an annual recertification to maintain PIERS access. This course provides refresher training on the Privacy Act, Personally Identifiable Information (PII) and proper handling of PII.

The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require users to agree to the rules to 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.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access.

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

The information collected, if exposed to unauthorized users may cause inconvenience, distress, or damage to standing or reputation and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraphs 8e are implemented to secure the data in the system in accordance with federal laws and policies, including Department policies.

9. Data Access

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

TRIP has the following National Passport Information Center (NPIC) users: Customer Service Staff, Customer Service Manager, Business Administrator, System Administrator and Database Administrator**.**

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

Access is determined based on position and roles which are approved by the supervisor and the local ISSO. TRIP users consist of both civilian and contract employees. User access is role based and granted only the role(s) required to perform assigned duties:

National Passport Information Center (NPIC) users:

Customer Service Staff: Users assigned to perform tasks as defined and approved, in addition to performing customer inquiry activities under the supervision of the Customer Service Manager.

Customer Service Manager: A Customer Service Manager (CSM) is responsible for responding to time sensitive and/or critical inquiries such as Congressional referrals and other urgent inquiries and implementing tracking mechanisms to ensure all notification requests are responded to in the required timeframes.

Business Administrator: Manages and maintains user profiles, including position and responsibilities.

System Administrator: Manages and maintains business rules, and other administrative functions such as maintaining reference data including inquiry types and site list. Also manage pre-defined queries designed for use across the enterprise and updates of user business rules implemented in the system.

Database Administrator: Responsible for the daily maintenance, upgrades, patch/hot fix applications, backups and configurations to the databases.

(**c**) **Are procedures, controls or responsibilities regarding access to data in the system documented?** ☒Yes ☐No

Information is documented in the TRIP System Security Plan. The Plan includes information regarding system access to data.

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

TRIP users other than administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and local ISSO approves to perform official duties.

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

-Access control policies and access enforcement mechanisms control access to PII.

-Separation of duties is implemented; access is role-based as required by policy.

-Least Privileges, which are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII via dual factor authentication utilizing a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN).

-Privacy training informs users of the Rules of Behavior and warns against unauthorized browsing.