PRIVACY IMPACT ASSESSMENT

Smart Traveler Enrollment Program (STEP)

1. Contact Information

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

2. System Information

(a) Name of system: Smart Traveler Enrollment Program (STEP)

(b) Bureau: Consular Affairs (CA)

(c) System acronym: STEP

(d) iMatrix Asset ID Number: 27

(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 – in routing for approval

(b) What is the security Assessment and Authorization (A&A) status of the system?

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

(c) Describe the purpose of the system:

The Smart Traveler Enrollment Program (STEP) is a free service that allows American citizens and nationals who are traveling to, or living in a foreign country to provide travel registration information electronically via the Internet. STEP allows travelers to enter information about their upcoming trip abroad so that the Department of State (DoS) can better assist them in an emergency. The Consular Task Force (CTF) component allows the Department of State to provide assistance and information to American citizens overseas when a crisis occurs. STEP allows Americans residing abroad to get routine information from the nearest U.S. embassy or consulate. Signing up for the program allows travelers to receive detailed information about their destination country. Travelers also receive situational updates, including Travel Warnings and Travel Alerts, which are essential news and warnings provided by the U.S. government about specific destinations.

The CTF component of STEP is used by the DoS to provide assistance and information to American citizens overseas when a crisis occurs. CTF provides the DoS the capability to create and maintain subject records of Americans potentially associated with a crisis at hand. The Task Force Alert (TFA) and the Evacuation and Repatriation Tool (ERT) are also components of the STEP boundary by way of CTF.

- TFA is a public-facing web application that allows the public to input information on American citizens potentially impacted by a crisis situation for which a Task Force has been established.

- The ERT allows U.S. Department of State Consular officials to enter data from Forms DS- 3072 (Repatriation/Emergency Medical and Dietary Assistance Loan Application) and DS-5528 (Evacuee Manifest and Promissory Note) submitted by U.S. Citizens requiring emergency services. The ERT tool is installed on a Toughbook laptop and not connected to STEP or any network.

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

To register a trip for temporary travel or overseas residence, travelers must enter their name, address, birthdate, place of birth, gender, marital status, other names, mother's maiden name, nationality/citizenship, phone number, email address, social security number, passport or other ID numbers, employment information, family information and one form of contact, such as their physical address, telephone number, and email address. Users have the option of registering their overseas residence and/or travel plans by entering the name of the country of residence or

destination and the physical address and/or telephone number of the in-country residence or lodging.

STEP prompts users to enter the following additional PII (optional) regarding a travel companion: name, birthdate, gender, and country of citizenship, relationship to registrant, passport information, address, telephone number and email address.

Department of State business information (DoS point of contact name, post, organization, phone, and email) is also collected on employees accessing STEP to perform duties.

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

- 8 U.S.C. 1101 et seq., Immigration and Nationality Act of 1952, as amended, including 8 U.S.C. 1104 Powers and duties of Secretary of State and 8 U.S.C. 1185, Travel Documentation of Aliens and Citizens
- 22 U.S.C. 1731 – Protection of Naturalized Citizens
- 22 U.S.C. 2651a Organization of Department of State
- 22 U.S.C. 2715 Procedures regarding major disasters and incidents abroad affecting United States citizens
- 22 U.S.C. 3904 Functions of service
- Executive Order 11295 of August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)

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

☒Yes, provide:

- SORN Name and Number:
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published 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 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

A-15-001-04a: Office of Overseas Citizen Services- Smart Traveler Enrollment Program (STEP)
Description: Hardcopy and Electronic Source Records: Original paper records and records on independent databases by posts for travel registration. If necessary for reasons of disability or inability to use the online site, a hard copy of the registration form can be filled out by a traveler and entered by authorized consular staff into the IBRS database.

Disposition: Temporary: Hold copies in file areas temporarily until transfer to IBRS is completed, after which the paper copies will be destroyed. Destroy/delete electronic data after verification of input into the system.

DispAuthNo: N1-059-06-09, item 1

A-15-001-04b: Office of Overseas Citizen Services - Smart Traveler Enrollment Program (STEP)
Description: Electronic Content Records. The Internet Based Registration System data base consists of two electronic data files that are retained on-line for access by users and/or OCS personnel. The data files are as follows: Individual Registration Files contain electronic personal information about Americans taking short trips (six months or less), longer trips or residing overseas including their home address, contact information, passport information, emergency contact information, and travel itinerary. Organizational Representative Files contain electronic information about the agent or organization who serves as point of contact making arrangements for other travelers (e.g., universities, churches, travel agencies, etc.). These electronic records are kept open and active until trip reported end date.

Disposition: Temporary: Cutoff after end of trip or last log on. Maintain individual registration and organizational representative data in active file for 12 months. Send e-mail to registrant advising of no trip or other activity for 12 months. Automatically delete data if no response to e-mail in three months. Automatically delete data for registrants with no e-mail address 15 months after notification. Indefinite term registrations of overseas residents are removed by post when no longer needed for reference.

DispAuthNo: N1-059-06-09, item 2

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>are</u> US citizens or aliens lawfully admitted for permanent residence)
☒ U.S. Government/Federal employees or Contractor employees
☒ Other (are <u>not</u> 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?

- Immigration and Nationality Act of 1952, as amended (8 U.S.C. 1101 et seq.):
- Title 22 U.S. Code Foreign Relations and Intercourse (various Chapters)
- Title 22 Code of Federal Regulations (CFR) (various parts, including, Parts 40 – 53 and Parts 96-99.)

(c) How is the information collected?

STEP is a public facing page which provide American citizens and nationals access to apply for services. STEP collects information electronically via the public website using DS-4024 Form, "Smart Traveler Enrollment Program." The information is collected from travelers and/or from third parties such as travel agents regarding travels to foreign countries. Additionally, consular officers or other consular personnel may create new registration records on a traveler's behalf if the traveler does not have access to the Internet or otherwise requests this service. The system is accessible by both public and DoS users.

Data entered into TFA by a public user is uploaded and stored in the TFA Oracle database within the DMZ. The CCD Exadata database then pulls the data from the DMZ into the CTF database.

Information in the ERT component is collected from applicants in person or via emails to posts. Information is manually keyed into the ERT tool by DoS staff from Forms DS-3072 (Repatriation/Emergency Medical and Dietary Assistance Loan Application) and DS-5528 (Evacuee Manifest and Promissory Note) submitted by U.S. Citizens requiring emergency services. The information from ERT is then uploaded to CTF via email.

(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?

Accuracy of the data in STEP and TFA is dependent on the individual user's registration process. It is the responsibility of each registrant to correct information entered incorrectly and to update information that was accurate when entered, but has since changed.

The applicant is responsible for ensuring the information provided for emergency services is accurate. That information is entered into ERT along with a scanned copy of the individual's passport. The passport is uploaded in machine readable format and validated against the data in ERT.

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

Ensuring the data is current is dependent on the individual users registering through STEP. It is the responsibility of each registrant to correct information that was entered incorrectly and to update information that was accurate when entered but has since changed. STEP users must create a user account and login to access their information again after it has been originally submitted. Individuals who have an account may delete, amend, or supplement the information they provide at any time by logging into their online STEP account.

It is the individual users' responsibility to ensure the information entered in TFA is current. Since it is public facing, individuals are able to provide additional or new information for the duration of the task force.

The information entered into ERT creates a manifest for emergency services. That manifest is exported to CTF and validated against CCD to ensure the information is current.

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

STEP does not use commercial or publicly available information.

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

Yes, notification is provided to individuals prior to collection of PII information. Before a user is allowed to create an account on the STEP system, there is a prominently displayed Privacy Act Statement and a box the user checks indicating it has been read.

(i) **Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?** ☒Yes ☐No

Opt-In Consent. STEP has a prominently displayed Privacy Act Statement and a box the user checks indicating it has been read.

-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 items listed in Question 3d are the minimum necessary to perform the actions required by the STEP system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration.

5. Use of information

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

The intended use of the PII in STEP is to support the State Department's protection of and service to U.S. citizens and nationals abroad.

(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 of the Consular Affairs American Citizens Services. Applicants' PII and information in STEP regarding upcoming trips abroad are used to provide alerts regarding conditions in the country and to assist them in case of an emergency.

(c) Does the system analyze the information stored in it? ☐Yes ☒No

STEP does not analyze the information stored.

(1) Does the analysis result in new information? ☐Yes ☐No

(2) Will the new information be placed in the individual's record? ☐Yes ☐No

(3) 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.

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 STEP system will be shared internally with the CA system Consular Consolidated Database (CCD) to support and provide integrated information to the Consular Affairs staff that provide travel and crisis services to U.S. Citizens abroad. Data collected and stored by the STEP system components are replicated to CCD, where the ACS system pulls the replicated data from CCD for use by post personnel abroad.

Externally: No information is shared externally via STEP.

(b) What information will be shared?

The PII listed paragraph 3d is shared with CCD to perform the function for which it was intended, which is to provide services and information to American citizens and nationals traveling abroad or in a crisis situation abroad.

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

The PII is used and shared within internal CA organizations so that the traveler can be contacted in the event of an emergency and to provide required CA services as needed.

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

The secure protocol Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS) is used to access the STEP for the purpose of conducting consular business. Communications between STEP and CCD is database to database and is encrypted using Transport Layer Security (TLS).

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

STEP uses HTTP and HTTPS and Transmission Control Protocols (TCP) to transport data across the network with the internal CA CCD system listed in paragraph 6e above. The TCP protocol suite consists of multiple layers of protocols that help ensure the integrity of data transmission. Additionally, the server to server connection between the STEP and CCD servers is protected using Transport Layer Security (TLS).

(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 non-authorized parties
b. Deliberate disclosure/theft of information regardless whether the motivation was monetary, personal or other.

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.

These risks are mitigated using a multi-faceted approach to security:

- Frequent security training for all State Department personnel and contractors regarding information security, including the safe handling and storage of PII, classification levels, including “Sensitive but Unclassified,” and signing a user agreement.

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

- A system authorization and accreditation process along with continuous monitoring (Risk Management Framework (RMF)). 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?

STEP users must create a user account and provide a user name and password to log into the system initially. They can access their information again after it has been originally submitted using their password. Individuals who have an account may delete, amend, or supplement the information they provide at any time by logging into their online STEP account.

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

☒Yes ☐No

If yes, explain the procedures.

STEP users can access their information after it has been originally submitted using their log-on information. Individuals who have an account may delete, amend, or supplement the information they provide at any time by logging into their online STEP account.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information? Individuals are notified of the procedures to correct records in STEP by the following methods:

The STATE-26 Passport Records (March 24, 2015) and STATE-05, Overseas Citizens Services Records and Other Overseas Records (September 8, 2016) provides guidance on procedures to correct information.

The STEP enrollment site provides procedures on how to update and correct account information.

Each method contains information on how to amend records and contact information.

8. Security Controls

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

The system is secured through the use of defense in depth - layers of security including 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 official duties.

Access to applications is controlled at the application level; there are additional access controls at the database level. All accounts for the STEP system must be approved by the user's supervisor and the Information System Security Officer. The audit vault system is used to monitor all privileged access to the system in which audit logs are viewed at the application, database, and system level for abnormal activities. Users are uniquely identified and authenticated while logged in and activity can be traced to the person performing specific activities. Any violations are reported to senior management, if applicable for appropriate action.

Access to STEP by the public is restricted to the application(s) submitted using the account created.

(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.

Internal access is limited to authorized users of the Department of State's unclassified network, including cleared contractors who have a justified need for the information in order to perform official duties. Authorization to the network requires a background investigation and an application approved by the supervisor and the local Information System Security Officer. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been 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 and is required for logon, in addition to unique passwords to access STEP.

Applications are configured according to the State Department Security Configuration Guides to to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (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. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

Access to the 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 Information System Security Officers (ISSOs) determine the access level needed by a user (including managers) to ensure it correlates to the user's job function and clearance level.

(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 configuration guides. They also 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 Department of State network connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

Connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State 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 (PS800 Cyber Security Awareness) training is required for all authorized users. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. PA318 (Protecting Personally Identifiable Information) privacy training is required for all OpenNet users biennially.

(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 and implemented in accordance with NIST 800-53 and Department of State Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired.

Data in transit are encrypted. Physical and environmental protection is implemented, and media handling configuration management is utilized. 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. Dual factor authentication is required and implemented to identify and authenticate users accessing STEP in accordance with Department of State and federal guidelines.

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

Due to the sensitivity of information collected, information is secured by effective procedures for access authorization.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, 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 8a-e are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

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

The following groups are STEP users: Public users (self-enrollment), Department of State (DoS) users (Overseas Consular users, Overseas Citizen Services, and CTF users), Step Administrator, System Administrators and Database Administrators. Users consist of both civil service and contractor personnel.

- **Public Users**- Public users are American citizens and nationals who sign up for the STEP services.
- **DoS STEP Users** – DoS users consist of consular case workers and users to manage posts' data to assist U.S. citizens and domestic users for oversight and reporting purposes.
- **STEP Administrator** – Maintains travel information and frequently asked questions functionality and validate posts functionality.
- **System Administrator** – Responsible for daily maintenance, establishing access control lists (ACLs), maintaining user accounts and backups.
- **Database Administrators** – Responsible for daily maintenance, upgrades, patch/hotfix and database configuration.

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

Access is determined based on requests submitted by the supervisor and approved by the local ISSO. Access is role-based and user is granted only the role(s) required to perform officially assigned duties.

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

The STEP System Security 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.

Public users will have access to only the data they submit to the STEP application via their logon authentication.

Users will not have access to all data in the system outside of administrators. Access to information is role-based. Separation of duties and least privilege are 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.

-Least Privileges 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 STEP PII via dual factor authentication that is required to access and log on to a federal system.