

STEP 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:** Smart Traveler Enrollment Program

(b) **Bureau:** Bureau of 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):**

N/A

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?**

In accordance with the Federal Information Security Management Act (FISMA) of 2002, the assessment and authorization of this system is underway. STEP is expected to receive an Authorization To Operate (ATO) in July 2015. This document was updated as part of the reauthorization of the system.

(c) **Describe the purpose of the system:**

STEP allows travelers to enter information about their upcoming trip abroad so that the Department of State can better assist them in an emergency. STEP also allows Americans residing abroad to get routine information from the nearest U.S. embassy or consulate. Signing up for the program is easy, and travelers can then receive detailed information about their destination country. Travelers also receive any updates, including Travel Warnings and Travel Alerts, which are essential news updates and warnings provided by the U.S. government about specific destinations. STEP allows government authorities to contact and assist travelers during emergencies, political violence, or natural disasters.

(d) **Describe the PII that the system collects, uses, maintains, or disseminates:**

Users have the option to create and modify their own account in STEP or to register a single trip without an account. To create an account with STEP, users must provide:

- Username
- Password
- Security question
- Security question answer

To register a trip or overseas residence in STEP (with or without an account), users must provide:

- Traveler's first name
- Traveler's last name
- Traveler's date of birth
- At least one form of contact information such as physical address, telephone number or email address.

In addition, during the registration process, STEP prompts users to enter their passport information as well as the name, address, telephone number and email address for one emergency contact. However, this information is not required to complete the registration process.

Once the traveler's personal information has been provided, users have the option of registering their overseas residence and/or travel plans. To do so, users must provide the following required information:

- Name of country of residence or destination
- Date of arrival in that country
- Address or phone number of in-country residence or lodging

STEP prompts users to enter the following additional information (optional):

- Date of departure from the country
- Description of duration of stay
- Description of purpose of visit
- Travel companion information including:
 - Name
 - Date of birth
 - Gender
 - Country of citizenship
 - Relationship to user
 - Passport information
 - Address, telephone number and email address

STEP does not collect any additional data from users by means of persistent tracking technologies (e.g., persistent cookies).

The Task Force Alert (TFA) component of Consular Task Force (CTF) collects the same PII from the public that STEP does.

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

- 8 U.S.C. 1401-1504(2013) (Nationality and Naturalization)

- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 U.S.C. 211a-218, 2651a, 2705 (2007); Executive Order 11295 (August 5, 1966) (Authority of Department of State in issuing, denying, or limiting U.S. passports)
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1104 (Powers and duties of Secretary of State)
- 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. 1731 (Protection to naturalized citizens abroad)
- 22 U.S.C. 3904 (Functions of service)
- 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance)
- 22 CFR Subchapter F, Nationality and Passports; Subchapter H, Protection and Welfare of Americans, Their Property and Estates; Subchapter J, Legal and Related Services; Subchapter T, Hostage Relief

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

Yes, provide:

- SORN Name and Number:
Passport Records, State-26, July 26, 2011
Overseas Citizens Service Records, State-05, May 2, 2008

If "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:

A-15-001-04a Office of Overseas Citizen Services - Smart Traveler Enrollment Program (STEP)

Description: a. 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 hard 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: b. 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

A-15-001-04c Office of Overseas Citizen Services - Smart Traveler Enrollment Program (STEP)

Description: c. Management and Operations Records

Documentation. File consists of all final formal deliverables placed into the Consular Systems Division Project Repository. This documentation includes the SRS, SDS, User Guide, Help Documentation, Programmer Maintenance Manual, and final reports (regardless of medium) relating to a master file or data base that has been authorized by GRS or a NARA-approved disposition schedule.

Disposition: TEMPORARY: Destroy or delete when superseded or obsolete, or upon authorized deletion of the related master file or data base, or upon the destruction of the last output of the system if the output is needed to protect legal rights, whichever is latest.

DispAuthNo: GRS 20, item 11a

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

Not applicable because STEP does not collect the traveler's SSN.

If yes, under what authorization?

(c) How is the information collected?

STEP collects information from persons who voluntarily provide it by accessing the Department of State's secure Internet web site registration page available at <https://step.state.gov>. Persons may register individually or through third parties such as travel agents. 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 paper application (DS-4024) can be found at the Department of State's e-Form website.

<http://www.state.gov/documents/organization/83011.pdf>

All enrollment information is automatically sent by STEP to the ACS system of the post with responsibility for the location(s) of the indicated travel. It is accessible to any ACS or CCD user with the appropriate access role and permission, such as consular officers and other consular personnel in other posts and in the Bureau of Consular Affairs, Overseas Citizens Services CA/OCS in Washington, D.C.

(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 is dependent on the individual user's registration process 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.

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

Accuracy of the data 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.

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

No. STEP uses only information entered by the STEP user/registrant.

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

Notice is provided to the user prior to collection of their information. STEP requires the user to complete the Privacy Act notification. Registrants are required to indicate that they have read the Privacy Act statement before registering a trip.

(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?

U.S. citizens have the right and opportunity to decline to provide the information requested. However, services may be contingent upon their explicit acceptance of the terms. American citizens who utilize STEP may specify the categories of persons with whom the information may be shared. The categories are: Family Members, Friends, Legal Representative, Media, Medical Representative, Members of Congress.

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 required personal data collected by STEP is limited to travelers' names, dates of birth, contact information and locations of travel. It is the minimum necessary to carry out the function of STEP. The STEP application data is protected by multiple layers of security controls including OpenNet security, STEP application security, Department site physical security and management security.

5. Use of information

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

The data collected through STEP is used to contact U.S. citizens in the event of an emergency, to disseminate travel alerts and warnings, emergency and security messages, post newsletters, and other information relevant to the U.S. citizen community living or traveling abroad. The information can also be sorted by posts to manage their contact lists.

New data or previously unavailable personal data will be created through derived data or aggregation of data collected in STEP. However, records created within the STEP system are available in the Consular Consolidated Database (CCD). Once this data is aggregated in CCD, it serves as both a backup for each post's transaction activity and it enables Consular Affairs management to apply advanced metrics against the data. Whenever a record is updated within STEP, the information is replicated into the CCD where it is maintained.

Consular Users have the ability to generate predefined reports of the STEP travel data entered by the registrants based upon selected criteria. Reports are used to help Consular Users manage the registration records in the STEP system, especially in the event of an emergency.

(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.

(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?**

N/A

(2) Does the analysis result in new information?

N/A

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

N/A

(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

N/A

6. Sharing of Information**(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.**

The information is used and shared within internal organizations so that the traveler can be contacted in the event of an emergency.

The information may be shared externally with: Family Members, Friends, Legal Representative, Media, Medical Representative, and Members of Congress.

Access to STEP data is restricted to Department of State OpenNet Users who have appropriate permissions as follows:

- CA authorized STEP System Administrator
- Overseas Consular employees working in the American Citizen Services section
- Domestic Users in the Bureau of Consular Affairs' Directorate of Overseas Citizen Services, Office of American Citizen Services
- Consular Affairs Administrative Users (Web/System/Database)
- Transportation carriers and wardens living within the consulate district affected by a crisis

(b) What information will be shared?

The personally identifiable information collected by STEP is shared solely within the Bureau of Consular Affairs, among cleared employees with role-based access to the data and is done so via secure transmission methods.

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

The information is used and shared within internal organizations so that the traveler can be contacted in the event of an emergency.

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

No agencies external to CA have access to the data in STEP. Occasionally, limited personal information is shared with third parties described in 6c and 6e for the purpose of properly responding to a crisis.

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

Consular officers and other personnel may, from time to time and on an as-needed-basis, share information obtained from STEP with third parties where necessary to preserve the health and safety of American citizens as indicated in the Overseas Citizens Services System of Records Notice, STATE-05 and Passport Records, STATE-26.

Such parties may include transportation carriers and wardens living within the consulate district affected by a crisis. Carriers are provided only the minimal personal information necessary to respond to the crisis. Information is generally supplied pursuant to a Memorandum of Understanding governing the use of the information.

Wardens are provided only the minimal personal information necessary – usually name and contact information – to allow them to pass along information to the U.S. citizen. Information is transmitted to wardens by hardcopy whenever possible, and must be returned by wardens upon completion of their tenure.

Each warden is required to sign a memorandum of understanding governing the use and security of personal information provided by the Department of State.

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

The risk to privacy of sharing information obtained through STEP with participants of the warden system is that the information provided will be used for unauthorized purposes, lost, stolen or misappropriated. The risk is mitigated by requiring a memorandum of understanding from the warden, providing only hardcopy whenever possible, and requiring that hard copy be returned by wardens upon completion of their tenure.

7. Redress and Notification

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

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.

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

Yes

No

If yes, explain the procedures.

Refer to 7(a).

If no, explain why not.

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

STEP is covered by the Privacy Act, and this is documented during the creation of the user account, therefore formal procedures for notification and redress exist.

8. Security Controls

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

The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and tested and implemented those controls to ensure that the controls continue to work properly.

(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.

Adequate controls to limit access and to regulate the behavior of authorized users are implemented in STEP. 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 detect and deter 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.

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

STEP keeps track of the create/last update date for each of the data elements stored in the database. This provides traceability for each user that has updated/created an item and when the item was updated / created. In addition STEP also provides a "Notes" functionality that provides an audit trail for updates made to Subjects, Related Subjects, and Contacts. The notes are system-generated based on updates that are made to each individual record and can be exported from the application when needed. The application is role-based and allows access to different data elements/functionality based on the role of the user accessing the applications.

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

All personnel accessing systems residing on the OpenNet or OpenNet Plus are required to attend the following two security awareness-raising presentations:

- Diplomatic Security’s Security Briefing
- Consular Affairs’ in-house Security Awareness presentation
- The Department requires all direct-hire employees who handle personally identifiable information (PII) while performing their official duties to satisfactorily complete the

Foreign Service Institute (FSI) distance learning course PA459, Protecting Personally Identifiable Information (PII). The training is not mandatory for contractors but they are permitted to take the course.

- Additionally, all Department employees must take and pass an annual Cyber Security Awareness Training course, which includes elements of privacy training, in order to retain access to the Department's unclassified network,

Both presentations require signed acknowledgement of the rules of behavior and include segments covering appropriate system usage and formal statements on the Rules of Behavior regarding Department of State computer systems.

Once a CA employee user has been provided OpenNet access, they are required to attend CA specific security awareness training. All CA users are required to take two types of security training:

- Information Security (INFOSEC) Briefing - New CA users are required to attend a site-specific security briefing within 30 days of joining the Bureau.
- OpenNet Plus Online Training. Users who have taken this online training with another Bureau within the last year do not need to take the training again until after their one-year anniversary date. All other users are required to take the training within 5 days of receiving a CA logon.

Failure to take either training course can result in revoking a user's access to the Bureau's Information Systems.

(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 STEP security and privacy controls in place are adequate to safeguard customer privacy. STEP utilizes numerous management, operational and technical security controls to protect the data in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). 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 (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports.

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

Security measures are set commensurate with the data which is stored, processed, and transmitted within the STEP system.

9. Data Access

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

STEP Administrators and Overseas Consular Users have access to the data in the system.

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

Access to the data for STEP is controlled through the use of user accounts with login and password requirements, and the use of roles.

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

Yes No

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

The STEP Internet site allows Public Users to:

- Sign up for Travel Warnings and Travel Alerts issued by the Department of State via email for a country of choice
- Register trips and residence abroad online

STEP public users will only have access to their own data which they input into the system. The data they input will be used to provide travel warnings and / or notify them in the event of an emergency.

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

- All Consular Users, including external agency users, are screened prior to their employment with the Department or their respective agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before given access to any CA/CST system via the State Department secure intranet, including STEP, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.
- It is mandatory for all Department of State employees and contractors to pass 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.
- Each domestic organization has at least one Consular Systems administrator who is responsible for managing the non-public users within the organization. Consular Systems administrators are government employees who use the Consular Shared Tables-Administrator (CST-Admin) application to approve account requests and assign STEP roles appropriate for each user's job requirement. STEP roles determine what a non-public user can do on STEP.

- The Consular Systems administrator determines the access level to CA applications controlled by Consular Shared Tables (CST) needed by a non-public user (including managers) to ensure it correlates to the user's particular job function and level of clearance. Contractors who support STEP are subject to a rigorous background investigation by the contract employer and are checked against several government and criminal law enforcement databases for facts that may bear on the loyalty and trustworthiness of the individual. At the very minimum, contractors involved in the development and/or maintenance of STEP hardware and software must have a level "Secret" security clearance. Once the highest-level background investigation required has been completed, cleared technical personnel (government and contractors) will be allowed to access the server rooms housing STEP.