PRIVACY IMPACT ASSESSMENT

Consular Affairs American Citizens Services (CAACS)

1. Contact Information

<table>
<thead>
<tr>
<th>A/GIS Deputy Assistant Secretary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bureau of Administration</td>
</tr>
<tr>
<td>Global Information Services</td>
</tr>
</tbody>
</table>

2. System Information

(a) Name of system: Consular Affairs American Citizens Services
(b) Bureau: Consular Affairs (CA)
(c) System acronym: CAACS
(d) iMatrix Asset ID Number: CAACS 258561; ATS 720; IPCA 39; STEP 27; CTF 4696 (child to STEP)
(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. CAACS is expected to receive an ATO in Summer 2018.
(c) Describe the purpose of the system:
   Consular Affairs American Citizen Services (CAACS) is a logical business grouping of application systems which consists of: Adoptions Tracking Service (ATS), International Parental-Child Abduction System (IPCA), and Smart Traveler Enrollment Program (STEP).
   
   **ATS:** The Adoptions Tracking Service (ATS) supports the U.S. Central Authority’s (USCA’s) day-to-day operations and helps the USCA meet its responsibilities by collecting, storing, and retrieving adoption-related information. It allows its users to report on adoption-related issues and activities and to communicate electronically with domestic and foreign individuals and organizations who provide adoption-related services.
The Adoptions Tracking Service also supports the collection of information about the organizations and individuals who provide inter-country adoption services. It facilitates the communication and reporting of adoption case information to a broad audience, including other State Department offices, other governmental agencies, non-government adoption-related organizations, members of the public, and members of Congress. The Adoptions Tracking Service also supports:

- Automatic importing of adoption-related immigration case data from external systems
- Electronic collection of adoption-related immigration and emigration case data from the organizations and individuals who provide adoption services
- Electronic collection of information that allows the USCA to oversee and monitor organizations and individuals that provides adoption-related services
- Retrieval and reporting of USCA adoption-related information

**IPCA:** The International Parental Child Abduction System (IPCA) tracks information about international parental child abductions from the initial stage through final resolution by the courts. The application tracks all documents, correspondence, and legal proceedings, and allows journal entries to be tracked by caseworkers. The Bureau of Consular Affairs Overseas Citizens Services Directorate, Office of Children’s Issues (CA/OCS/CI) at the Department of State assists parents, attorneys, other government agencies, and foreign governments in the return of children abducted by their parents and prevention of future international parental child abductions. CA/OCS/CI shares the information collected in IPCA with the Federal Bureau of Investigation (FBI), other federal agencies, the International Police Organization (INTERPOL), and foreign governments as required. The IPCA software is used only by CA/OCS/CI within the Department of State. CA/OCS/CI is responsible for the management and tracking of information related to international parental child abduction cases and potential cases, including their related subjects, action items, legal proceedings, documents, notes and so forth.

**STEP:** The Smart Traveler Enrollment Program (STEP) allows American citizens 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 can better assist them in an emergency. The role of the STEP application is to accept information from American citizens through the Internet via appropriate secure connections. 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 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. The CTF component provides DoS the capability to create and maintain subject records of Americans.
potentially associated with the crisis at hand. STEP allows government authorities to contact and assist travelers during emergencies, political violence, or natural disasters.

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

**ATS:** ATS collects the following information on U.S. citizens, non-U.S. citizens, and U.S. government employees: name, gender, address, phone number, marital status

The adoption service provider (ASP) handling the case collects the name, gender, date of birth, country of birth, citizenship, and visa file number of non-U.S. citizen children who are adopted to the United States from the person or entity with legal custody of the child. For children being adopted from the United States, the ASP or state adoptions authorities collect the child’s name, gender, date of birth, country of birth (U.S.), and citizenship status.

The Hague Complaint Registry portion of ATS collects the complainant’s name, address, home phone, type of violation being reported, and a description of the nature of the complaint being registered. Complainants may also enter work phone number, email address, name of the adoptions service provider and adoptions agencies involved; name and nationality of the child involved, U.S. destination of the child; any applicable law enforcement information, including the agency’s name, point of contact at the agency, street address, telephone number; or applicable state licensing agency information, including the agency’s name, point of contact at the agency, street address, and telephone number; and additional comments the complainant would like to make.

**IPCA:** IPCA collects the following information on U.S. citizens, non-U.S. citizens, and U.S. government employees:

- Department of State employee assigned to the case: name, relevant business contact information.

- Left-Behind-Parent (LBP): name, birthdate, birthplace, passport and visa information for LBP, relatives, attorney of record for the LBP.

- Taking Parent (TP): name, birthdate, birthplace, passport and visa information, if available, contact information, specific location (if available), known relatives, attorney of record for the TP.

- Missing Child: name, birthdate, birthplace, SSN, passport and visa information if available, circumstances of abduction.

- Case: Sensitive documents such as birth certificates, child custody agreements, divorce decrees and other legal documents are uploaded and stored in the application.
STEP: To register a trip for temporary travel or overseas residence travelers must enter their name, birthdate, and one form of contact, such as their physical address, telephone number, and email address. Travelers may also enter passport information. 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.

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

- 8 CFR Part 204 Immigrant Petitions
- 8 CFR Part 213a Affidavits of Support on Behalf of Immigrants
- 18 U.S.C. 1073 – Fugitive Felon Act
- 22 U.S.C. 211a-218, 2705; Passports and Consular Reports of Birth Abroad of a U.S. Citizen
- 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. 2670j Provision of emergency medical, dietary and other assistance
- 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)
- 22 CFR Subchapter F, Nationality and Passports, including 22 CFR 51.28, Minors; Subchapter H, Protection and Welfare of Americans, Their Property and Estates; Subchapter J, Legal and Related Services, including Part 94, International Child Abduction and Part 96, Inter-country Adoption Accreditation of Agencies and Approval of Persons; Subchapter T, Hostage Relief

- 22 CFR 42.24 Adoption under the Hague Convention on Protection of Children and Cooperation in Respect of Inter-country Adoption and the Inter-country Adoption Act of 2000
- 42 U.S.C. 14901 et seq. - Inter-country Adoption Act of 2000
42 U.S.C. 14925 - Inter-country Adoption Universal Accreditation Act of 2012

(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 24Mar2015
  STATE-05 Overseas Citizens Services Records and Other Overseas Records 8Sep2016

☐ No, explain how the information is retrieved without a personal identifier.
Enter Text if applicable

(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: (obtain info from http://infoaccess.state.gov/recordmgt/recdispsched.asp)
(If the list is long – name only the top level and indicate length of time as variable based on document and detailed info is at the link)
- Schedule number (e.g., (XX-587-XX-XXX)):
- Length of time the information is retained in the system:
- Type of information retained in the system:

A-13-001-12a: Passport Records Access and Disclosure Request Files
Description: Case files created in response to requests for information (Passport Records) under the Freedom of Information Act (FOIA), Mandatory Declassification Review (MDR) process, Privacy Act, Classification Challenge, and similar access programs: Includes requests (either first-party or third-party); replies; copies of requested records; administrative appeals; related supporting documents (such as sanitizing instructions).
Note 1: Record copies of requested records remain covered by their original disposal authority, but if disposable sooner than their associated access/disclosure case file, may be retained under this item for disposition with that case file.

Note 2: Agencies may wish to retain redacted copies of requested records for business use after the rest of the associated request case file is destroyed.
Disposition: Temporary. Destroy 6 years after final agency action or 3 years after final adjudication by courts, whichever is later, but longer retention is authorized if required for business use.

DispAuthNo: DAA-GRS-2016-0002-0001 (GRS 4.2, item 020)

A-15-001-04: Office of Overseas Citizen Services- Smart Traveler Enrollment Program (STEP)
Description: The Office of Overseas Citizen Services has developed a web-based database that allows citizens to register their travel plans on-line. The database is accessible by both the OCS and all American embassies and consulates world-wide, but is kept and maintained behind Department firewalls in the Enterprise Sever Operations Center (ESOC) by IRM. Registration allows Americans to record information about their upcoming trips abroad so that the Department of State can provide information and assistance in case of emergency. Americans residing abroad may also receive routine information from the U.S. embassy or consulate for which they are registered. All information requested is covered under the Privacy Act System of Records State 05, Overseas Services Records.

The database system to this point has kept all information received from registrants and has yet to archive information. While this database is independent, information collected and maintained within it is also transferred via electronic interface to the American Citizen Service plus (ACS+) database, which includes American citizen data outside of travel information. This data is used not only for security purposes in the case of an emergency, but can also be used for statistical purposes, and to track consular services to American citizens overseas. The Internet-Based Travel Registration System (IBRS) is the predecessor system to STEP. The IBRS system was implemented in June 2004.

Disposition: Temporary: See sub sections 01a - c for specific dispositions.
DispAuthNo: N1-059-06-09

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.

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.

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

A-15-002-02: Child Custody/Abduction Case Files
Description: Cases reflect applications filed for the return of children abducted to countries that are party and not party to the Hague Abduction Convention. Included are requests for assistance in locating children taken by the other parent, legal proceedings, information of available courses of action, monitoring the welfare of a child, information on child custody laws and procedures in the host country, and related correspondence.

Disposition: Transfer to the RSC after the case is deemed closed and no action has taken place for 1 year for transfer to the WNRC. Destroy when 15 years old.
DispAuthNo: N1-059-97-14, item 2

A15-002-03: Adoptions Tracking Service (ATS)
Description: ATS is an electronic information system designed to track, monitor, and report on all adoption cases involving emigration from or immigration to the U.S as mandated by the Intercountry Adoption Act of 2000 (IAA). Activities include monitoring organizations that provide inter-country adoption services, responding to adoption-related inquiries from the public and other interested stakeholders, reporting to Congressional representatives on inter-country adoptions involving U.S. citizens, producing mandatory annual reports to Congress, and communicating with all inter-country adoption stakeholders.

ATS supports the U.S. Central Authority for Inter-country Adoptions (USCA), which has inter-country adoption-related responsibilities involving U.S. citizens. The IAA designated the Department of State as U.S. Central Authority for Inter-country Adoptions under the Hague Adoption Convention. The day-to-day work of the U.S. Central Authority is the responsibility of the Bureau of Consular Affairs, Directorate of Overseas Citizens Services, Office of Children’s Issues (CA/OCS/CI).

ATS records include the following types of information: unique identifier, case status and tracking information, application information, adoptive parent information, child information, Hague Convention documentation, inquiry and complaint information, and adoption agency information.

Disposition: Temporary. Cut off at end of calendar year when adoption case closes. Destroy 75 years after adoption case closed
DispAuthNo: N1-059-09-09, item 1

4. Characterization of the Information
(a) What entities below are the original sources of the information in the system?
Please check all that apply.
☒ Members of the Public (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?
  ● Inter-country Adoption Act of 2000 (42 U.S.C. 14901 et seq.)
  ● Inter-country Adoption Universal Accreditation Act of 2012 (42 U.S.C. 14925)
  ● 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?
CAACS contains two public facing pages (ATS and STEP) which provide American citizens access to apply for services.

**ATS:** General public ATS information is collected via its public facing page via the web. The accrediting entities (AE) and adoption service providers (ASP) also enters information via the web. The general public issues complaints via the use of the Hague Complaint Registry (HCR) web component. The system is accessible by both public and OpenNet users. The AE and adoption providers provide information directly into the ATS.

**IPCA** is an internal tracking database where information is collected by the case worker by various means e.g., face-face, court records, etc., and entered into the system. IPCA maintains information on U.S. citizens, non-U.S. citizens, and U.S. government employees. IPCA maintains the same information on children and parents involved in an international abduction, regardless of the child’s citizenship status. Information is initially collected from the left behind parent (LBP). Once a case is opened, the information is supplemented with legal documentation from the LBP and/or his attorney via various means such as phone, fax, email, face-to face etc., and any additional relevant information from Consular Affairs (passport and visa records). The CA/OCS/CI caseworker then gathers relevant information from law enforcement sources and international databases on the taking parent (TP) and missing child. All data is stored in the IPCA database. The system is accessible by OpenNet users.

**STEP** collects information from citizens 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 OpenNet users.
(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?

**ATS:** The accuracy of the information about adopted children and adoptive parents is verified by the USCA through ASPs and state adoptions authorities and communication with adoptive parents. HCR data relies upon the complainant entering the data. Once entered, the data is viewed by DoS employees in CA/OCS/CI and matched to the case being referenced in the complaint.

**IPCA:** The information in IPCA is checked for accuracy by the caseworker assigned to each case. The caseworker verifies the parent-child relationship and any other family data through various documentation requests, such as court orders or other legal documents from the LBP and/or attorneys of record. Additionally, CA/OCS/CI reviews appropriate passport and visa records and contacts federal/state law enforcement agencies directly involved, such as Interpol U.S., and the U.S. mission in the country where the child was allegedly abducted.

**STEP:** 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?

**ATS:** The AE and ASP users, along with USCA users in CA/OCS/CI, are responsible for verifying the relevance of HCR and adoptions case data. Any inconsistencies in the information contained in ATS can be clarified by communication with the relevant parties, including but not limited to the complainant or the ASP handling the case.

**IPCA:** IPCA’s information is input based upon information provided to the DoS representative by victims of international parental child abductions. The data is current when input and is updated as the case progresses to closure. After the case is closed, there is no need to update the information. If PII needs to be updated while the case is open, the parent/legal representative would notify the caseworker who can update the system.

**STEP:** 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.

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

**ATS:** Does not use commercial or publicly available information.

**IPCA:** IPCA uses information collected from members of Congress, foreign governments via diplomatic notes, foreign Central Authorities under the Hague Convention, state and federal court records and other interested parties with information relevant to locating the missing child, including the left-behind parent and his/her attorney and non-governmental organizations (NGOs) (non-profit agencies). Occasionally, information is gathered from foreign court records, foreign government agencies and ministries, and foreign NGOs. IPCA uses this information to create a comprehensive case file on a missing child and relevant family members.

**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 in accordance with the following requirements regarding US Citizens and/or legally admitted permanent residents (green card holders):

1) The Department must have a Privacy Policy – and the system must have a link to it
2) The system must have a Privacy Act Statement – on the web page that collects PII
3) Forms, whether paper or electronic, must have a Privacy Act Statement on them

The following applies to the CAACS application systems:

**ATS:** No notice is provided to adopted children; however, all forms relevant to ATS used by USCA, AEs, and ASPs to collect data from adoptive parents and other sources contain a Privacy Act Statement (PAS), which indicates what information is collected, the purpose for the collection, with whom the information will be shared, and the consequences of not providing the data requested. System of Records Notices STATE-05 and 26 are also published in the Federal Register and provide the public notice as to the type of information collected in ATS. Although some initial information may be entered into ATS for inter-country adoptions, the application is completed, printed, signed, and sent in via fax or U.S. Mail.

**IPCA:** IPCA is not public facing and is accessed only by OpenNet personnel; a PAS is not required.

**STEP:** 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

**ATS:** Implied. A Privacy Act Statement is provided on the home page of ATS. Consent is implied when the user clicks to continue and fills in the information.

**IPCA:** IPCA is not public facing and is not accessed by the public. Consent is not required for this system which is accessed only by OpenNet personnel. Forms the applicant may complete have a PAS on the form.

**STEP:** Opt-In Consent. System 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 this 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 CAACS is to support the State Department’s abductions and adoptions work, protection of and service to U.S. citizens abroad, and for visa processing in connection with the adoption process for lawful immigrants and visitors traveling to the United States.

(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 system which is to provide International Parental-Child Abduction System (IPCA), Smart Traveler Enrollment Program (STEP) and Adoption Tracking Service (ATS) capabilities and services to American Citizens.

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

The system does not analyze the information stored in it. Rather, it generates reports that may be analyzed by authorized users.
ATS: Reports on adoptions status can be produced with Parent/Spouse Surname, Child Surname, Adoptions Type (Immigration, Emigration, All) on them. Authorized ATS users, based on the user’s role in the system, have access to reports on individuals, which are used primarily in the ATS mission of tracking inter-country adoptions. Some reports, as mandated, are directed to the U.S. Congress.

IPCA: All IPCA reports are selected and run from the IPCA Reports screen. On this screen, users select the type of report and any report criteria necessary to retrieve the desired information. Such reports are used to review and document the details of a specific case. Only authorized users, based on the user’s role, would have access to these reports. Routine statistical reports are generated on total counts of abduction/access cases by country for use by the Overseas Citizens Services Directorate (CA/OCS) management, CA/OCS/CI Abduction Unit, Department principals, and Congress. These reports are available to relevant interested parties, including foreign governments. Data and/or case summaries provided to relevant interested parties would be contingent upon obtaining a Privacy Act Waiver (PAW) allowing dissemination of case specific data.

STEP: No analysis occurs

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.

ATS: Internally: Consular Consolidated Database (CCD); Immigrant Visa Overseas (IVO)
External: Data is shared with the AE/ASP component which is public facing. This data is also shared with other government agencies and Congress through annual reporting and ad hoc reports upon request.

IPCA: Internally: CCD; Consular Shared Tables (CST)
External: Information stored in IPCA may be shared manually (not by system connection) with external law enforcement, foreign governments, Congress, other federal agencies and non-governmental organizations to help locate or facilitate the return of an abducted child. The information collected in IPCA is also shared with the FBI,
INTERPOL, other federal agencies, and foreign governments as the cases progress and actions or collaboration with other legal and governmental entities become necessary.

Note: The uses of the IPCA information by external entities are in accordance with relevant statutory authority and purpose, such as the National Child Search Assistance Act of 1990 (NCSA), specifically, 42 U.S.C. § 5779 (Reporting Requirement) and 42 U.S.C. § 5780 (State Requirements). The NCSA requires local, state and federal law enforcement agencies, when informed of an abduction, to immediately enter the appropriate data into the National Crime Information Center (NCIC) database without requiring a waiting period. Sharing the information that is necessary to help locate an abducted child with relevant law enforcement agencies is considered a "routine use" and permitted under the NCSA.

**STEP:** Internally: CCD; American Citizen Services (ACS)
Externally: None

(b) What information will be shared?
The following CAACS PII is shared to perform the function for which it was intended, i.e., adoption tracking, missing children, information about Americans traveling abroad. The data being collected is listed below:

- Names of Individual
- Birthdates of Individual
- Financial Account Numbers of Individuals
- Social Security Numbers
- Phone number(s) of Individuals
- Business Address(es)
- Personal Address
- e-mail address(es) of individuals
- Substantive individual legal information
- Substantive individual personnel information
- Substantive individual family information
- Other substantive individual information

**ATS/STEP:** All PII listed above may be shared with CCD and CST.
ATS External sharing: All PII outlined in paragraph 6.(b), may be shared with other governmental agencies, non-government adoption-related organizations, members of the public, and members of Congress.

**IPCA:** All of the above PII is necessary for the agency/agencies to perform the tasks of locating missing children, and that which is in accordance with the NCSA. There is an IPCA lookup report on the CCD that can be accessed by authorized individuals. Additionally, IPCA data is stored on the CCD in the CA/OCS database.

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

**ATS:** ATS information is shared internally with the Consular Consolidated Database (CCD), and any information that is entered into ATS by users is replicated to the CCD. All data sharing is for the purpose of processing, monitoring, safeguarding and reporting on the inter-country adoptions process. External information shared provides updates pertaining to adoption case information for reporting purposes to Congress and to assist agencies and persons of interest such as lawyers and parents with up-to-date status information.

**IPCA:** Information is shared internally within the State Department, other government agencies, foreign and domestic organizations and individuals who have a need-to-know because they are participants in the process or implementers of the decisions. Information is shared internally within the State Department to address and resolve children’s issues such as locating and facilitating return of an abducted child, the whereabouts of parents, etc. Information shared with external agencies consist of information regarding the whereabouts of parents and abducted children as needed by U.S. domestic and foreign law enforcement organizations. U.S. domestic and foreign child welfare NGOs or lawyers representing either parent needs information regarding case status and case decisions. Information is provided to these entities by officials acting on behalf of the Department of State via emails, letters, phone calls, in-person meetings or diplomatic notes.

**STEP:** 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?

**ATS:** Data transmitted to and from ATS is protected by the bulk encryptions inherent within OpenNet that encrypt the data from posts to the CCD database. CA uses a secure protocol and non-secure protocol to access CA’s Web Sites for the purpose of conducting consular business. The secure protocol connection provides strong encryption (128-bit) and with some applications,
user/client authentication is also required. AE/ASP access is encrypted via a PKI certificate issued to each authorized user to access ATS data via the internet.

**IPCA:** Information shared internally is via CCD. External sharing of information is by paper, secure email, phone call, letter, in-person meetings, and diplomatic notes.

**STEP:** CA uses a secure protocol and non-secure protocol to access CA’s Web Sites for the purpose of conducting consular business. The secure protocol connection provides strong encryption (128-bit) and with some applications, user/client authentication is also required.

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

**ATS:** An Interface Control Document (ICD) is used to define and disclose transmission formats via OpenNet. The interfaced systems are strictly controlled by firewalls and Network Intrusion Detection Systems (NIDS) rules that limit ingress and egress to the ATS. All changes are requested from the Firewall Advisor Board (FAB) using a Universal Trouble Ticket (UTT). Each UTT is vetted by technical personnel and management prior to the change being implemented. Access to electronic files is protected by Personal Identity Verification/Personal Identification Number (PIV/PIN), and is under the supervision of system managers. Additionally, audit trails monitoring computer usage and access to files are frequently reviewed. Finally, regularly administered security/privacy training informs authorized State Department and federal users of the proper handling of data, and of privacy and security issues. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA) formally signed by Authorizing Officers of each Agency.

**IPCA:** IPCA is restricted to system/database administrators, users in the Office of Children's Issues (CA/OCS/CI) and the Criminal Investigative Liaison office that supports CA/OCS/CI at the Department of State. IPCA is accessed via OpenNet. OpenNet's security controls include firewalls and Network Intrusion Detection Systems (NIDS) which limit the risk of unauthorized access. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA) formally signed by Authorizing Officers of each Agency.

**STEP:** Consular officers and other personnel may, from time to time and on an as-needed-basis, share information obtained from STEP with third parties such as transportation carriers and wardens living within the consular district affected by a crisis to preserve the health and safety of American citizens as indicated in the Overseas Citizens Services Records and Other Overseas Records System of Records Notice, STATE-05 and Passport Records, STATE-26. Data provided is the minimal personal information necessary to respond to a 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 provide information to the U.S. citizen. Information is provided to wardens by hardcopy in person 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?

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, “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 (RMF)). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

- All communications shared with external agencies are encrypted as to protect the data prior to transmission.

7. Redress and Notification

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

ATS: ATS applicants can log on and see information about them in the system; however, they cannot change many fields. They can update contact information.
IPCA: Parents do not have access to the system. They can access information via contact with the DoS representative, caseworker, or by contacting the Director, Office of Information Programs and Services, Bureau of Administration, A/GIS/IPS, SA-2, Department of State, Washington, DC 20522.

STEP: STEP users must create a user account and log in 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.

Individuals are notified of the procedures to correct records in these systems by a variety of methods: each method contains information on how to amend records and who/what office to communicate with as well as contact information.

ATS/IPCA: Persons with PII in ATS or IPCA must contact the Overseas Citizens Services Directorate (CA/OCS) if CA/OCS has records pertaining to them or should write to the Director, Office of Information Programs and Services, A/GIS/IPS, SA–2, Department of State, Washington, DC 20522

STEP: STEP users must create a user account and log in 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.

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 these systems by a variety of methods:

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

- The IPCA enrollment site provides procedures on how to correct information. Also information is provided during the applicant’s interview.
The STEP enrollment site provides procedures on how to update and correct account information.

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

8. Security Controls

(a) How is the information in the system secured?
The system is secured within the Department of State intranet, OpenNet, where risk factors are mitigated 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.

(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 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.

Applications are configured according to the State Department Security Configuration Guides to optimize security Configuration Guides 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 are noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

A system use notification (“warning banner”) is displayed before logon is permitted and informs the user of system use and restrictions with every login. Users are required to read and actively click a button indicating understanding and agreement before logon can be completed.

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. Security Officers determine the access level needed by a user
(including managers) to ensure it correlates to the user’s 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 configuration guides, 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 OpenNet-connected systems that host CA’s major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g. administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

Access control lists on all OpenNet servers and devices along with Department of State 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 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.

Operating System (OS)-Level auditing is set in accordance with the Department of State Security Configuration Guide. The OS interface allows the system administrator or ISSO to review audit trail information through the security log found in the event viewer. In addition to the security log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is
authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

The OS interface-based auditing provides for some specific actions:

- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

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

In accordance with Department of State computer security policies, mandatory annual security training, which has a privacy component, is required for all authorized users. Each user must complete the Cyber Security Awareness Training annually and pass the PA-459 course “Protecting Personally Identifiable Information”. The Department’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

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 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. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

(f) How were the security measures above influenced by the type of information collected?
Based on an awareness that the consequence to organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, or damage to standing or reputation, financial loss, harm to Department programs or the public interest, unauthorized release of sensitive information, threats to personal safety, and/or civil or criminal violation, the security measures listed above were implemented to secure the data in the system.

9. Data Access

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

**ATS**: Users of ATS can be broken down into four basic types of users: OpenNet-based Users, Public Users, System Administrators, and Database Administrators.

**OpenNet users:**

- **United States Central Authority (USCA) users** - State Department personnel accessing ATS via OpenNet who are responsible for responding to general inter-country adoption-related issues and specific inter-country adoption case information requests from Congressional staff, prospective parents, adoption service providers, and others.

- **CST Administrator** - The CST administrator creates and manages the ATS user IDs and passwords for all ATS users except for AE/ASP and HCR users (Public Users).

- **Web Administrator** - The Web Administrator creates and manages the ATS web server account that each internet user must log into when establishing an ATS web session.

- **System Administrator/Database Administrator** - The System and Database Administrators include both government employees and contractors. They are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration, to the database.

**Public users:**

- Adoption Service Provider users and Accrediting Entity (AE) users access ATS via an internet web server. They are responsible for supplying a variety of inter-country adoption-related information.

**Pre-Adoption Immigration Review (PAIR) User**

- Hague Complaint Registry (HCR) User

**PAIR USERS**: Users access ATS via an internet web server and are authorized to view, create, edit, and delete a portable document format from a PAIR Record. There are five types of PAIR users:

- **USCIS - U.S. Citizenship and Immigration Services**
• NBC - USCIS National Benefits Center (Lee’s Summit, Missouri)
• NVC - Department of State’s National Visa Center (Portsmouth, New Hampshire)
• Addis Ababa (Ethiopian Post)
• Taipei (Taiwan Post)

**HCR users** access ATS via the HCR public web site without authentication and may only enter new complaints to the registry.

**IPCA:** Users include OpenNet users; Web/Database/System administrators.

- **OpenNet** - CA/OSC/CI employees to manage active abduction cases and maintain a central repository on all documentation relating to an open case.

- **Web Administrator** - The Web Administrator creates and manages the IPCA web server accounts that each user must log into when establishing an IPCA web session.

- **Database Administrator** - Database Administrators (DBA) are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration, to the database.

- **System Administrator** - The System Administrators include both government employees and contractors.

**STEP:** Public users (self-enrollment information), System Administrators, Overseas Citizen Services Domestic Users and Overseas Consular Users have access to the data in the system.

(b) How is access to data in the system determined?
Access is determined based on requests which are approved by the supervisor and 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
Information is documented in the 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.
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 is employed and users have access to only the data that the supervisor and 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. Concerning PII, 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 (CAC/PIV and PIN).