PRIVACY IMPACT ASSESSMENT

Consular Affairs (CA) Adoptions Tracking Service (ATS)

1. Contact Information

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

2. System Information

(a) Name of system: Adoptions Tracking Service
(b) Bureau: Consular Affairs (CA)
(c) System acronym: ATS
(d) iMatrix Asset ID Number: 720
(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 Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. ATS is expected to receive its ATO in Summer 2021.

(c) Describe the purpose of the system:

The U.S. Department of State is the U.S. Central Authority (USCA) for the Hague Convention on the Protection of Children and Co-operation in Respect of Intercountry Adoption (Hague Adoption Convention). The Bureau of Consular Affairs, Directorate of Overseas Citizens Services, Office of Children's Issues carries out most of the day-to-day functions of the USCA. The USCA oversees the accreditation and approval of adoption service providers providing services in intercountry adoptions, and it communicates with foreign countries as well as domestic and international organizations regarding intercountry adoption issues

Adoptions Tracking Service (ATS) is an internet-based system that adoption service providers and accrediting entities use to provide information on intercountry adoptions to the U.S. Department of State. ATS supports USCA's day-to-day operations by electronically collecting, storing, and retrieving intercountry adoption-related information. It allows 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 USCA relies on the ATS system to:

- Help USCA monitor and oversee the accredited agencies and approved persons who provide intercountry adoption services;
- Electronically collect intercountry adoption-related immigration and emigration case data from the accredited bodies and approved persons who provide adoption services;
- Create and maintain Pre-Adoption Immigration Review (PAIR) records;
- Track information related to complaints submitted through the Hague Complaint Registry (HCR) website via the Travel State Government (TSG) website, which is outside the boundary of ATS;
- Automatically import intercountry adoption-related immigration case data from Department of State Visa systems: Immigrant Visa Overseas (IVO) and the Immigrant Visa Information System (IVIS) via the Consular Consolidated Database (CCD);
- Respond to inquiries from the public and other interested parties about intercountry adoptions;
- Communicate with all intercountry adoption stakeholders, including other State Department offices, other governmental agencies, non-government adoption-related organizations, members of the public, and members of Congress;
- Report to Congress on intercountry adoptions involving U.S. citizens; and
- Provide information about the USCA's work to carry out its mission.

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

ATS contains the following PII on U.S. citizens and non-U.S. citizens: name, personal phone number, personal email address, personal address, date of birth, place of birth, nationality, family information, gender, citizenship status, marital status, Social Security numbers and U.S. passport information and other forms of official government identification that constitute national identification.

ATS also collects the following business contact information associated with the intercountry adoption process: Names of organizations and agencies, point of contact names, emails, work addresses and phone numbers.

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

- 22 U.S.C. 2651a Organization of Department of State
- 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
- 22 CFR 42.24 Adoption under the Hague Convention on Protection of Children and Co-operation in Respect of Intercountry Adoption and the Intercountry Adoption Act of 2000
- 22 CFR 96.43

- 22 CFR 99.2

(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-39 Visa Records June 15, 2018
  STATE-05 Overseas Citizens Services Records and Other Overseas Records September 8, 2016

☐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 Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

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 USCA, which has inter-country adoption-related responsibilities involving U.S. citizens. The IAA designated the Department of State as the USCA under the Hague Adoption Convention. The day-to-day work of the USCA 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?

- Intercountry Adoption Act of 2000 (42 U.S.C. 14901 et seq.)
- Intercountry Adoption Universal Accreditation Act of 2012 (42 U.S.C. 14925)
- 26 U.S.C. 6039E - Information Concerning Resident Status

(c) How is the information collected?

ATS collects information via its public-facing page from accrediting entities (AEs) and adoption service providers (ASPs), the Hague Complaint Registry (HCR) and the Pre-Adoption Immigration Review (PAIR) officials. The AE/ASP/HCR/PAIR users access state.gov and connect to the ATS Web Server via a COTS web browser running on their non-Department of State owned/managed workstation. The user is directed to the AE, ASP, HCR, or PAIR user web home page based on their assigned responsibility. The AEs, ASPs, and PAIR users provide information directly into ATS. ATS allows 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 general public issues complaints into ATS via the use of the Hague Complaint Registry (HCR) web component through the Travel State Government (TSG) website. TSG is is outside the boundary of ATS.

The following Department of Homeland Security (DHS)/U.S. Citizenship and Immigration Services (USCIS) forms are used in the adoption process in which information is provided to DHS/USCIS by the applicant: DHS/USCIS Forms I-800-A Application for determination of Suitability to Adopt a Child from a Cenvention Country; I800-A, Supplement 1, Listing of Adult Member of Household, I800-A Supplement 2, Consent to Disclose Information; Supplement 3, Request for Action on Approved Form I-800A; G-1145, E-Notification of Application/Petition Acceptance. DHS provides relevant information to the AEs and ASPs to assist with the cases, in which they enter information into the ATS to monitor and track adoption cases.

(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?

The accuracy of the information in ATS about adopted children and adoptive parents is verified by the USCA through ASPs, state adoptions authorities, and communication with adoptive parents. The Complaint Registry (CR) data rely upon the complainant entering the data accurately. Once entered, the data are viewed by Department of State (DoS) employees in CA/OCS/CI and matched to the case referenced in the complaint.

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

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 in ATS. 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.

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

ATS 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. A Privacy Act Statement is provided on the source forms in which DHS/USCIS, accrediting entities (AEs) and adoption service providers (ASPs) collect information. Additionally, the ATS home page contains a Privacy Act Statement. Consent is implied when the user clicks to continue and fills in the information.

System of Records Notices STATE-05, 26, and 39 are also published in the Federal Register and provide the public notice as to the type of information collected in ATS.

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

A Privacy Act Statement is provided on the home page of ATS and applicable forms. Consent is implied when the user proceeds to provide the information.

-If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?

The PII listed in Question 3d is the minimum necessary to perform the actions required by ATS. 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 PII in ATS is used to:

- Validate applicants suitability of adoption and provide adoption services;
- Track adoptions from Convention Countries;
- Review, assess and accredit AEs and ASPs to participate in the Hague Convention process to provide intercountry adoption services; and
- Report to Congress on intercountry adoptions involving U.S. citizens.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. The PII provides ATS information to track and manage intercountry adoptions and required Congressional reporting. ATS also supports the collection of information about organizations and individuals who provide intercountry services.

(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.

Various reports on adoptions status are produced to support daily operations of USCA staff. These include reports by parent/spouse surname, child surname and adoptions type. 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 intercountry adoptions. Some reports, as mandated, are provided to the U.S. Congress.

(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.

Internal Information Sharing:

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, ATS receives information from the Immigrant Visa Overseas (IVO) system and the Immigrant Visa system (IVIS) via the Consular Consolidated Database (CCD). Information in ATS is replicated and maintained in the CCD.

External DoS Information Sharing: Data are shared with the AEs and ASPs via the ATS public-facing website on State.gov. This data is also shared with other government agencies such as the Departmetn of Health and Human Services, DHS, and Congress. The agencies involved depends on the circumstances of the case. Information may also be shared with non-government adoption-related organizations and authorized members of the public via reports, correspondence, emails, and telephone calls.

(b) What information will be shared?

The PII in paragraph 3(d) above is shared. Other information shared includes: intercountry adoption-related immigration and emigration case data from the accredited bodies and approved persons who provide adoption services; Pre-Adoption Immigration Review (PAIR) records; and information about the USCA's work to carry out its mission.

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

The ATS data are shared to monitor, safeguard and report on the intercountry adoptions process..

Externally-shared information provides agencies and persons of interests such as lawyers with up-to-date status information. Information is also shared externally with Congress for reporting purposes.

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

Internally: To access ATS, DoS employees must have a Verification/Personal Identification Number (PIV/PIN), in addition to a separate unique user ID and password to access data. Data are transmitted within DoS database to database.

Externally: Data are transmitted via Transport Layer Security (TLS) v1.2, externally to AEs, ASPs, and PAIR users via onsite workstations where DoS users are authenticated to ATS using both their individual State-Public Key Infrastructure (PKI) identification certificate and their individual ATS webserver password. The DoS user is directed to the AE, ASP, HCR or PAIR home page depending on their approved and assigned responsibility. Data are shared with other government agencies via CCD. Information is shared with non-governmental adoption-related organizations and authorized members of the public via reports, correspondence, emails, and telephone calls.

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

ATS uses the secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS) which provides secure encryption interface with the CCD, in addition to user/client authentication. The interface is controlled by firewalls and Network Intrusion Detection Systems (NIDS) rules that limit ingress and egress to ATS. All communication between the ATS Desktop client and OpenNet Database server is encrypted using Transport Layer Security.

Internal sharing: To access ATS DoS employees must have a Verification/Personal Identification Number (PIV/PIN), in addition to a separate unique user ID and password to access data. All data between ATS and CCD are encrypted using transport layer Security. Use of ATS is under the supervision of system managers and local Information System Security Officers (ISSOs). Additionally, audit trails monitoring computer usage and access to files are frequently reviewed.

External sharing: ATS is an internet-based system that allows adoption service providers (ASPs), accrediting entities (AEs), and Pre-Adoption Immigration Review (PAIR) users to provide information on intercountry adoptions to the U.S. Department of State. AEs are designated by the Department of State to perform certain duties relating to the accreditation and approval of ASPs. ASPs must be accredited or approved by the AE prior to accessing ATS.

In order to maintain ATS security, the DoS grants access to ATS only to specific representatives of ASPs through an access application process. AE/ASP users must have browser encryption using Transport Layer Security settings in accordance with DoS specifications enabled on web browsers to connect to ATS for information sharing. Public Key Infrastructure (PKI) certificates are issued that authenticate the identity of users who access ATS data via the internet. Applicants must also accept and agree to the ATS Rules of Security Behavior. Once access is granted a PKI security certificate for access to ATS is provided.

Data are shared with other government agencies via CCD using secure transmission methods (Transmission Control Protocol (TCP) and Hypertext Transfer Protocol (HTTP)) approved by State Department policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Department of State has Memorandums of Understanding/Agreement (MOU/MOA) and Information Security Agreements (ISA) formally signed by Authorizing Officers of each Agency addressing the use and protection of information.

(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:

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

2) Deliberate disclosure of information to unauthorized parties or theft of information regardless whether the motivation was monetary, personal or other.

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

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, “Sensitive but Unclassified,” and all higher levels of classification. Users must also sign a user agreement.

2) Strict role-based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level.

3) System authorization and accreditation process along with continuous monitoring via the 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.

4) All communications shared with external agencies are encrypted in accordance with the Department of State's security policies and procedures.

7. Redress and Notification

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

The servicing AE or ASP can assist individuals in accessing information in the ATS system. Additionally, individuals can follow the Department's Privacy Act guidance on the public website and the guidance in STATE-26 Passport Records, STATE-05 Overseas Citizens Services Records and Other Overseas Records, and STATE-39, Visa Records, regarding procedures to access information.

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

☒Yes ☐No

If yes, explain the procedures.

Following are the procedures to correct records in the ATS system by a variety of methods; each method contains information on how to amend records as well as contact information.

- Information is provided during the adoption process by the AE or ASP on how to correct inaccurate information.

- Persons with PII in ATS can contact the Overseas Citizens Services Directorate (CA/OCS) to correct their information.

- Persons can contact the offices listed in STATE-26 Passport Records, STATE-05 Overseas Citizens Services Records and Other Overseas Records, and STATE-39, Visa Records, to correct inaccurate or erroneous information.

If no, explain why not.

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

ATS does not collect information from the individual directly. Information is collected via DHS/USCIS and the AE or ASP and submitted into the ATS. Procedures to correct information are provided during the adoption process by the AE or ASP.

The SORNs STATE-26 Passport Records, STATE-05 Overseas Citizens Services Records and Other Overseas Records, and STATE-39 Visa Records provide procedures on offices to contact to correct information.

8. Security Controls

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

ATS 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.

ATS is configured according to the State Department Bureau of Diplomatic Security Configuration Guides to optimize security while still providing functionality (compliant with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes 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.

(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 to ATS 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 agree to the user access agreement/rules of behavior before being given a user account. Authorized users are issued a Personal Identity Verification /Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement. In addition, data are transmitted externally to AEs and ASPs through the ATS website where users are authenticated to ATS using both their individual State-Public Key Infrastructure (PKI) identification certificate and their individual ATS webserver password.

Access to the system is role-based, and restricted according to approved job responsibilities and managerial concurrence. Access control lists restrict individuals to only perform functions within ATS approved for their specific role. Local Information System 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.

Adoption Service Provider (ASP) users must be accredited or approved by the Department of State (DoS) designated Accrediting Entity (AE) prior to accessing ATS.

(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 Security Configuration Guides and conduct annual control assessments (ACA) to ensure that all systems/applications comply with Department of State and federal security policies.

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to access applications within ATS. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also 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; and
- Changes in file access restrictions.

The purpose of the audit trail is to document modification of and/or unauthorized access to the system.

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

In accordance with Department of State computer security policies, security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component to access or use systems. Additionally, Department of State personnel are required to take the course PA318 (Protecting Personally Identifiable Information) every two years. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they 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 reduce and mitigate the risks associated with internal sharing and disclosure, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides. Data in transit are encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access.

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

The consequences to organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, damage to standing or reputation, financial loss to the Department or individuals, 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 in paragraphs 8a-f were implemented in accordance with the National Institute of Standards and Technology (NIST) guidelines 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?

Users of ATS include the following: Department of State (DoS) Internal ATS Users, CST Administrator, Security Administrators, Web Administrator, System Administrators, Database Administrators and Public Users.

DoS Internal ATS users:

- **DoS ATS users** - State Department personnel accessing ATS consist of DoS general users, Office of Children's Issues (CI) personnel, USCA and Visa Office staff. These DoS users are responsible for responding to general intercountry adoption-related issues and specific intercountry adoption case information requests from Congressional staff, prospective parents, adoption service providers, and others.
- **CST Administrator** - The **CST Administrator** creates and manages ATS user IDs and passwords for all ATS users except for AE/ASP and HCR users (Public Users).
- **Security Administrators** – The Security Administrator manages the security of ATS including proper activation, maintenance, and use of security features.
- **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 are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration, to the database.
- **Pre-Adoption Immigration Review (PAIR) Internal DoS User:** Department of State's National Visa Center (Portsmouth, New Hampshire); Addis Ababa (Ethiopian Post) and Taipei (Taiwan Post)

Public users:

- **Adoption Service Provider (ASP) and Accrediting Entity (AE) users** - ASP and AE users access the ATS via an internet web server on Travel.State.Gov site. They are responsible for supplying a variety of intercountry adoption-related information.
- **Pre-Adoption Immigration Review (PAIR) User -** PAIR users access ATS via the public-facing web server and are authorized to view, create, edit, and delete a portable document format (pdf.) from a PAIR Record. PAIR users do not have access to AE/ASP functions. 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)
- **Complaint Registry (CR) User** – CR users access ATS via the CR public web site on Travel.State.Gov site. CR users may only enter new complaints to the registry.

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

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

The Adoption Service Provider (ASP) users and Accrediting Entity (AE) users must apply for and be assessed and approved via the Hague Accreditation process prior to accessing ATS.

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

Information is documented in the ATS System Security Plan. The plan includes information and procedures 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.

Internal user:
Department of State (DoS) 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 their local ISSO approves to perform official duties.

PAIR Internal DoS users (DoS National Visa Center Portsmouth & New Hampshire) and Addis Ababa (Ethiopian Post) and Taipei (Taiwan Post) have access to PAIR records to create, edit, and delete iformation. No PAIR user has access to any of the AE/ASP functions.

External users:
PAIR DHS/USCIS users have access to see PAIR records via CCD to create, edit and delete information. Hague Complaint registry users may only enter new complaints to the registry.

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

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

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

-Least privileges which are restrictive rights/privileges or accesses needed by users for the performance of specified tasks is implemented. 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), PKI and their unique password. Activities while logged in can be traced to the person who performed the activity.