1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: August 10, 2010.

(b) Name of system: Adoptions Tracking Service

(c) System acronym: ATS

(d) IT Asset Baseline (ITAB) number: 720

(e) System description (Briefly describe scope, purpose, and major functions):

ATS tracks and reports on all adoptions cases immigrating to and emigrating from the United States. ATS supports the United States Central Authority for Inter-country Adoptions (USCA), which has certain responsibilities involving children adopted into and out of the United States pursuant to the 1993 Hague Convention on Protection of Children and Co-Operation in Respect of Inter-Country Adoptions (the Adoptions Convention). ATS supports the collection of information about organizations and individuals that provide inter-country adoptions services as well as adoptive families and adopted persons. The data maintained in ATS is used in the communication and reporting of adoptions case information to a broad audience of stakeholders, including other Department of States (DoS) offices, other U.S. Governmental agencies, non-government adoptions-related organizations and members of the public and their Congressional representatives.

Since 1993, over 80 countries have signed the Adoptions Convention. The convention's goal is to protect children involved in inter-country adoptions by establishing a central authority for inter-country adoptions in each signatory country. These central authorities establish and uphold standards for inter-country adoptions, facilitate communication between convention countries regarding inter-country adoptions issues, and accredit Adoptions Service Providers (ASPs).

The Inter-country Adoptions Act of 2000 (IAA) implements legislation for the convention in the United States, and establishes the Department of State as the U.S. Central Authority (USCA). The Department of State, as the designated USCA, has directed its Bureau of Consular Affairs Office of Children's Issues (CA/OCS/CI) to ensure that the U.S. Government complies with the Adoptions Convention.

The ATS provides the automated support needed to maintain information about ASPs and the Accrediting Entities (AEs) designated by the USCA to accredit the ASPs. The primary functions of the ATS, Version 02.00.01, are to: (1) maintain contact information about ASPs and AEs; (2) submit and track complaints via the

Hague Complaint Registry (HCR) web site; (3) track, monitor, and report on all inter-country adoptions to and from the United States; and (4) print Hague adoptions certificates and custody declarations.

ATS is installed in the DoS Office of Children's Issues (CA/OCS/CI) and users located at AEs and accredited ASPs only. The general public will be able to submit Hague Convention-related complaints through the HCR using a link on the Travel State Government (TSG) website, www.travel.state.gov, and HCR complaint registry form, also available via www.adoptions.state.gov.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification

(g) Explanation of modification (if applicable):

(h) Date of previous PIA (if applicable): October 1, 2009

3. Characterization of the Information

The system:

- ☐ does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

ATS collects the PII of U.S. persons who adopt children through the inter-country adoptions process (adoptions "applicants"), children adopted from the United States and children adopted to the United States (such children are not U.S. persons at the time the data is collected, but usually become U.S. persons thereafter). It also collects the PII of some persons employed with the USCS, the AEs and the ASPs.

A U.S. applicant's name, gender, address and phone number is collected from applicants directly and entered into ATS by ASP employees. In rare cases where a U.S. person residing in another country adopts a child from the United States, that applicant's name, gender, address, phone number, and marital status is collected by the ASP or state public adoptions authorities.

The names, gender, date of birth, country of birth, citizenship, and visa file number of children adopted to the United States is collected by the ASP handling the case 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 (United States), and citizenship.

The names and phone numbers of AE and ASP employees with access to ATS is also collected and maintained by ATS.

PII collected through the Hague Complaint Registry portion of ATS comes from the person filing the complaint. The following information must be provided for the web

form to be processed: (1) the complainant's first and last name; (2) mailing address, (3) home phone; (4) the type of violation being reported; and (5) a description of the nature of the complaint being registered. The following additional information is not required but may be entered: (6) complainant's work phone number; (7) complainant's email address; (8) the name of the adoptions service provider and adoptions agencies involved; (9) the name and nationality of the child involved; (10) the U.S. destination of the child; (11) any applicable law enforcement information including the agency's name, point of contact at the agency, street address, and telephone number; (12) any applicable state licensing agency information including the agency's name, point of contact at the agency, street address, and telephone number; and (13) any additional comments the complainant would like to make.

b. How is the information collected?

The information is collected by the Bureau of Consular Affairs, Office of Children's Issues (CA/OCS/CI) acting as the U.S. Central Authority (USCA) through case updates provided to them by the AEs and the ASPs through the use of the AE/ASP web component of ATS, and from the general public through the use of the HCR web component.

c. Why is the information collected and maintained?

ATS supports the collection of information about organizations and individuals that provide and consume inter-country adoptions services to enable the United States, through the USCA, to comply with its obligations under the Adoptions Convention and to ensure the integrity of the inter-country adoptions process.

To do so, ATS collects and maintains basic PII about the children being adopted, the adoptive parents, and the contact information for AEs and ASP employees assigned to each case. This allows the USCA to monitor each adoptions case, to respond to inquiries, and to investigate complaints.

d. How will the information be checked for accuracy?

The accuracy of the information about adopted children and adoptive parents is verified by 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 Children's Issues and matched to the case being referenced in the complaint.

The AE and ASP users, along with USCA users in the Office of Children's Issues, are responsible for verifying the relevance and accuracy 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.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

The system was developed and modified to support the Intercountry Adoptions Act of 2000 (IAA) and U.S. immigration and nationality law as defined in the major legislation listed below:

- 22 U.S. Code (various sections) Title 22 Foreign Relations and Intercourse
- 22 Code of Federal Regulations (CFR) (various sections) Title 22 Foreign Relations

-42 U.S.C. 14901, IAA, Section 102 (e) “Establishment of Registry”

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The ATS collects the minimum amount of PII necessary to complete its statutory functions described in Section 3(c) above. The ATS security and privacy controls in place are adequate to safeguard individual privacy. ATS 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.

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are generally limited to three categories. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft are:

- **Device theft or loss-** Lost or stolen laptops and other devices such as removable drives may contain PII.

- **Portable Devices-** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable Mp3 players creates risk by making PII easily transportable on devices that aren’t always properly secured.

- **Insider threat-** Disgruntled employees seeking revenge or inadvertent human error to send PII over the internet.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- 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

4. Uses of the Information

a. Describe all uses of the information.

ATS tracks and reports on inter-country adoption cases immigrating to and emigrating from the United States. ATS users use the information collected to: (1) maintain contact information about ASPs and AEs; (2) submit and track complaints via the Hague Complaint Registry (HCR) web site; (3) track, monitor, and report on all inter-country adoptions to and from the United States; and (4) print Hague adoptions certificates and custody declarations.

b. What types of methods are used to analyze the data? What new information may be produced?

Reports on adoption status can be produced having the following data about individuals:

- Parent/Spouse Surname
- Child Surname
- Adoption Type (Immigration, Emigration, All)

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.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

ATS shares data with the Consular Consolidated Database (CCD), a Department of State database. It does not share or obtain data with any other Government databases. All data sharing is for the purpose of processing, monitoring, safeguarding and reporting on the inter-country adoptions process.

d. Is the system a contractor used and owned system?

ATS is a Government-owned system. It is supported by contract employees. All employees and contractors undergo 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. Contractor owned facilities are annually inspected by the Department's Bureau of Diplomatic Security.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

The ATS performs basic internal analytical functions on the PII but does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no

risk of "function creep," wherein with the passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

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.

Contractors involved in the design, development and maintenance of ATS are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. All contractors involved in the development or maintenance of ATS hardware or software must have at least a Secret-level security clearance.

All employees (including Foreign Nationals working in embassies and consulates worldwide) and contractors undergo 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. Contractor owned facilities are annually inspected by Diplomatic Security.

5. Retention

a. How long is information retained?

The retention period for information in ATS varies based on the type of information in question. For a comprehensive listing, see Chapter 15 of the Department of State Records Disposition Schedule.

Paper records produced by this application are shredded or burned, per Departmetn of State record disposition schedules.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention can impact on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging. The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of ATS throughout the lifetime of the data.

All physical records containing PII are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) disposition schedules.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

ATS information is shared with the Consular Consolidated Database (CCD). 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.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

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. The Bureau of Consular Affairs (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.

An Interface Control Document (ICD) is used to define and disclose transmission formats via OpenNet. The Department of State systems that interface with ATS are strictly controlled by Firewall and NIDS rule sets 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.

All physical records are maintained in secured file cabinets or in restricted areas to which access is limited to authorized personnel and contractors. Access to electronic data is protected by passwords and is directly under the supervision of system managers.

The following safeguards are in place for each sharing arrangement:

All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel only. Access to electronic files is protected by passwords and is under the supervision of system managers. Additionally, audit trails to monitor computer usage and access to files are monitored. Finally, regularly administered security/privacy training informs authorized users of the proper handling of data, privacy, and security issues.

The ATS does not transmit information over non-government controlled lines.

Privacy rights for systems outside of ATS are the responsibility of the system manager, IT security manager, and/or privacy coordinator for those systems.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. ATS mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are

documented in sharing agreements. Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

To reduce the privacy risks, access to information is controlled by application access controls. Every server on CA OpenNet has NetIQ Security Manager installed, and it is used to monitor server activity. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal Department of State regulations.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The information in ATS is not shared with any external organization.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

N/A.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

N/A

8. Notice

The system:

☒ contains information covered by the Privacy Act. The information in this system is covered by *STATE-05, Overseas Citizen Services Records*, *STATE-26, Passport Records, and STATE-39, Visa Records*

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

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, which indicates what information is collected, why, for what purpose the information will be routinely used, who the information will be shared with, and the consequences of not providing the data requested. Notice is also published in the System of Records Notices STATE-5, 26 and 39.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes, though the individual is advised that failure to provide certain information may result in non-provision of the requested service or legal penalties.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Yes, the individual may choose not to provide some information. However, the individual is advised that failure to provide certain information may result in non-provision of the requested service or legal penalties. The HCR has mandatory fields which must be filled out for the system to process the complaint. Failure to populate each mandatory field will result in the inability to submit a complaint through the HCR system. Those mandatory fields are disclosed in Section 3(a) above.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

ATS complies with all Privacy Act requirements for notice at the point of collection. All online and paper forms used to collect information contain Privacy Act disclosures. Notice is also published in the System of Records Notices STATE-5, 26 and 39. The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. The privacy of adopted children is mitigated by the fact that only the minimal amount of PII necessary to track the adoptions is collected. Additionally, the USCA monitors and audits the adoptions services provided by ASPs to ensure the privacy of adopted children is protected. Therefore, this category of privacy risk is appropriately mitigated.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

ATS contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 7 above, and in rules published at 22 CFR 171.31. The procedures inform the individual how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport record on grounds pertaining to law enforcement, in the interest of national defense and foreign policy if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Since ATS is Privacy Act-covered, formal procedures for notification and redress exist. Therefore, this category of privacy risk is appropriately mitigated.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Access to the system is limited to authorized Department of State staff having a need for the system in the performance of their official duties, to AEs and accredited ASP entities with approved access, and to the general public for the Hague Complaint Registry. All authorized U.S. Government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network.

Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed for the performance of their official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g., curiosity browsing). Completed applications are also reviewed and approved by the information system security officer (ISSO) prior to assigning the logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

For AE and ASP users, authorized Local Registration Authority (LRA) in CA/OCS/CI communicate with the PKI Office for issuance of a PKI digital certificate. User access is "role-based," determined by the employee's supervisor. The level of access for the user restricts the data that may be seen and the degree to which data may be modified as noted.

Non-production uses (e.g., testing, training) of production data are limited by administrative controls.

b. What privacy orientation or training for the system is provided authorized users?

The Bureau of Consular Affairs (CA/CST) provides extensive training resources for ATS users. These resources include online training modules and short training videos. CA also offers in-person training for both small and large groups of users.

Additionally, all Department employees must take an annual Cyber Security Awareness Training course, which includes elements of privacy training.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Adequate controls to limit access and to regulate the behavior of authorized users are implemented in ATS. Therefore, this category of privacy risk is negligible. 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 deter and detect 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.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

ATS operates under standard, commercially-available software products residing on a U.S. government-operated computing platform not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in ATS.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No technologies commonly considered to elevate privacy risk are employed in ATS.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates ATS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the controls continue to work properly. In accordance with the Federal Information Security Management Act provision for the triennial recertification of this system, its most recent date of authorization to operate was February, 2008.