

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

### **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: October 1, 2009
- (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 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 Adoption (the Adoption Convention). ATS tracks and reports on all adoption cases immigrating to and emigrating from the United States. ATS supports the collection of information about organizations and individuals that provide inter-country adoption services and the communication and reporting of adoption case information to a broad audience of stakeholders, including other DoS offices, other governmental agencies, non-government adoption-related organizations and members of the public and their Congressional representatives.

Since 1993, over 60 countries have signed the Convention on Protection of Children and Co-operation in Respect of Inter-country Adoption. 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 will establish and uphold standards for inter-country adoption, and will facilitate communication between convention countries regarding inter-country adoption issues.

The Inter-country Adoption Act of 2000 (IAA) implements legislation for the convention in the United States, and establishes the USCA. The U.S. Department of State (DoS), as the designated U.S. Central Authority (USCA), has directed the Bureau of Consular Affairs Office of Children's Issues

**Privacy Impact Assessment: Adoptions Tracking Services (ATS)**

(CA/OCS/CI) to ensure that the United States government complies with the convention.

The ATS provides the automated support needed to maintain information about Accrediting Entities (AE) and Adoption Service Providers (ASP) inquiries related to these organizations. The primary functions of the ATS, Version 02.00.00 is to: 1) Maintain contact information about ASPs and AEs; 2) Inquiry management and tracking; 3) Provide the ability to submit and track complaints via the Hague Complaint Registry (HCR) web site; and 4) Ability to track, monitor, and report on certain intercountry adoptions to and from the United States.

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](http://www.travel.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): May 2008

**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?**

Information collected from Department of State (DOS) employees would be data relevant to the auditing of services provided, such as the employee’s name. Additionally, DoS employees working at the Office of Children’s Issues may input information about other American Citizens related to international

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

adoptions or the information may come from the Consular Consolidated Database (CCD).

Information collected from the general public via the Hague Complaint Registry portion of ATS includes the complainant's name, phone number, address, e-mail address, description of complaint, name and nationality of child involved, and law enforcement information (if applicable).

### **b. How is the information collected?**

The information is collected from the 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 inter-country adoption services and the communication and reporting of adoption case information to a broad audience of stakeholders, including other DoS offices, other governmental agencies, non-government adoption-related organizations and members of the public and their Congressional representatives.

The ATS provides the automated support needed to maintain information about Accrediting Entities (AE) and Adoption Service Providers (ASP) and inquiries related to these organizations. The primary functions of the ATS, Version 02.00.00 is to: 1) Maintain contact information about ASPs and AEs; 2) Inquiry management and tracking; 3) Provide the ability to submit and track complaints via the Hague Complaint Registry (HCR) web site; and 4) Ability to track, monitor, and report on all intercountry adoptions.

ATS information collected from Department of State employees would be data relevant to the auditing of services provided, such as the employees' name. Additionally, DoS employees working at the Office of Children's Issues may input information about others related to intercountry adoptions. Information collected from the general public via the Hague Complaint Registry portion of ATS includes the complainant's name, phone number, address, e-mail address, description of complaint, name and nationality of child involved, and law enforcement information (if applicable). Complaints are limited to issues regarding the Hague Convention and IAA policies, and issues regarding ASP and AE entities. Complaints registered through the HCR component of ATS are forwarded to the appropriate entity for investigation. For example, if the general public has an issue regarding the fees charged by a particular ASP, the complaint would be forwarded to the AE that is responsible for the oversight of the ASP in question. The AE would investigate the claim to determine if the ASP is at fault.

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

### **d. How will the information be checked for accuracy?**

The accuracy of the 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 users in the Office of Children's Issues, are responsible for verifying relevance and accuracy of HCR and adoption case data.

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

The system was developed and modified to support the Intercountry Adoption 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. The ATS security and privacy controls in place are adequate to safeguard customer privacy. ATS utilizes numerous management, operational and technical security controls to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. 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.

## **4. Uses of the Information**

### **a. Describe all uses of the information.**

ATS tracks and reports on certain adoption cases immigrating to and emigrating from the US. ATS supports the collection of information about organizations and individuals that provide inter-country adoption services and

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

the communication and reporting of adoption case information to a broad audience of stakeholders, including other DoS offices, other governmental agencies, non-government adoption-related organizations and members of the public and their Congressional representatives.

### **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 intercountry adoptions. Some reports, as mandated, are directed to the US Congress.

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

These applications use a secure protocol (SSL) and non-secure protocol to access CA's Web Sites for the purpose of conducting consular business. The secure protocol (SSL) connection provides strong encryption (128-bit) and with some applications, User/Client authentication is also required. ATS shares data with the CCD. All data sharing is for the purposes of completing the processing of the service.

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

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

### **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 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.**

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

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.

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 of records schedules, refer to Chapter 15 of the Department of State Records Disposition Schedule.

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

For virtually all ATS data, there is a limited lifecycle established by the records retention schedule. 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.

### **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 purposes of completing the processing of the service.

***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

**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. 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.

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.**

ATS personally identifiable information is shared solely within the Bureau of Consular Affairs, among cleared employees with role-based access to the data and is done so via secure transmission methods. As such, the privacy risk from internal sharing is negligible.

**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?**

No.

**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.
- does NOT contain information covered by the Privacy Act.

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

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

All forms contain a Privacy 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 exercise 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.

### **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. . The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses. 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.

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

### **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 Complaint Registry. All authorized 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 official duties. The user access agreement includes a 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. For AE and ASP users, authorized Local Registration Authority (LRA) in CA/OCS/CI before forwarding to 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 Office of Consular Systems and Technology 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.

## ***Privacy Impact Assessment: Adoptions Tracking Services (ATS)***

**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 government-operated computing platforms 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.