DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Adoptions Tracking Service (ATS)

Updated May 20, 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

A. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) **Does this system collect, maintain or disseminate personally identifiable information about individual members of the public**?**

2) **Does a Privacy Act system of records already exist?**

   YES _X__   NO___

   If yes, please provide the following:
   Overseas Citizen Service, Number: State -05
   Visa Records, Number: State -39

3) **What is the purpose of the system/application?**

   ATS supports the U.S. Central Authority for Inter-country Adoptions (USCA), which has inter-country adoption-related responsibilities involving U.S. citizens. 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 Department offices, other governmental agencies, non-government adoption-related organizations and members of the public and their Congressional representatives.

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

   The ATS provides the automated support needed to maintain information about Accrediting Entities (AE), Adoption Service Providers (ASP) and Adoption Authorities (AA) inquiries related to these organizations. The primary functions of the ATS are to: 1) Maintain contact information 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 all international adoptions.

4) **What legal authority authorizes the purchase or development of this system/application?**

   The system was developed and modified to support 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; and - 22 Code of Federal Regulations (CFR) (various sections) Title 22 Foreign Relations

C. <u>DATA IN THE SYSTEM:</u>

1) What categories of individuals are covered in the system?

- U.S. Citizens:

- Non-U.S. Citizens:

- DoS employee name is collected and stored with the applicant's record (as it relates to the auditing of actions taken during the processing of the applicant's service request).

2) What are the sources of the information in the system?

a. Who/what is the source of the information?
The primary sources of information are the Office of Childrens Issues, the AEs, the ASPs, and from the general public (for the HCR portion only). The DoS users at the Office of Childrens Issues input data into ATS that comes from the Bureau of Consular Affairs Consular Consolidated Database (CCD).

b. What type of information is collected from the source of the information?

Information collected from Department of State employees is data relevant to the auditing of services provided e.g. employees' names. Additionally, DoS employees working at the Office of Children's Issues may input information about others related to international 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).

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

The accuracy of the HCR data relies upon the complainant who enters 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 Office of Children's Issues users is responsible for verifying relevance and accuracy of HCR and adoption case data.

b. How will data be checked for completeness?

The accuracy of the HCR data is dependent upon the complainant who enters the data. Once entered, the data is viewed by DoS employees in the Office of Childrens Issues and matched to the case being referenced in the complaint. The Office of Childrens Issues is responsible for verifying relevance and accuracy of HCR and adoption case data.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

Data will be updated as new/updated information is acquired from the ASP, AE or the general public through the HCR during routine/regular contact.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

The use of the data is both relevant and necessary to the purpose for which the system is being designed; the data elements are described in the Data Dictionaries for the system.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

The AE's updates to contact information, milestone dates data from ASPs, and updates and comments from the Office of Children's Issues.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

The system can make determinations about DoS employees or members of the public that would not be possible without the new data.

4) Will the new data be placed in the individual's record?

The new data will be placed in the individual's record.

5) How will the new data be verified for relevance and accuracy?

The Office of Childrens Issues is responsible for verifying relevance and accuracy of adoption case data.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Once data is authenticated, an authorized system user can retrieve a record by searching using any of the following data:
- Parent/Spouse Surname;
- Child Surname;
- ID Number;
- Milestone;
- Adoption Type (Immigration, Emigration, All);
- Verification Status; and
- Date Range.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Reports on adoption status can be produced by 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 international adoptions. Some reports, as mandated, are directed to the U.S. Congress.

E. **MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:**

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

Consular Affairs employs configuration management controls over the software used to process registrant data. Databases that contain registrant data are under strict control of the Data Engineering team that ensures data integrity and database reliability.

2) **What are the retention periods of data in this system?**

The disposition schedule for records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

   The application is not using technologies in ways that the Department has not previously employed (e.g., monitoring software, Smart Cards, Caller ID).

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

   N/A

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

   The application can be used to identify individuals through the use of basic biographic information. The application can be used to monitor employee activity as it relates to the auditing of the process.

   Auditing data, such as an employee name, is collected for the purposes of auditing the process. Access to audit reports is limited to management personnel. Audit reports are only available to the Bureau of Consular Affairs management personnel.

7) **If the system is being modified, will the Privacy Act System of Records Notice require amendment or revision? Explain.**

   An amendment or revision to the existing System of Records Notices is not necessary.

8) **Are there forms associated with the system?   YES _X__   NO ___**
   If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

Official forms used to collect adoption case data entered into the application under this program are OMB approved and contain a Privacy Act statement. Specific information regarding how the data is used is contained in the System of Records Notices (State-05 and State-39).

F. ACCESS TO DATA:

1) **Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?**

Other than HCR public users inputting their own data, the primary users who access the data are DoS civil service personnel, adoption service providers, and accrediting entities, and contractors who may function as systems administrators. Developers may have access to data for the purpose of troubleshooting system and/or database problems.

2) **What are the criteria for gaining access to the system?   Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access is determined based on the user role. User roles are assigned by the local systems administrator based on the job the employee is performing. Only system administrators are allowed to assign user roles. HCR users access only the data they have input to the system. The criterion for gaining access to the system is documented.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**

HCR users can access only the data they have input into the system.
Other users will only have access to the data granted to the role that they have been assigned.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials.)**

All users are exposed to basic information system security awareness material before authorizing access to the application. Annually, all OpenNet users are required to take and pass a Cyber-Security Awareness Test.

All ATS domestic end-users utilize the *ATS Users Manual.*

Access to data in ATS is determined based on the user's role. An employee user role may allow access to all or only partial data in an applicant record. Some, but not all, access to records is audited. The primacy focus of an audit trails is to document the actions taken in processing a particular request for service, in particular the adjudication and printing of a citizenship document.

Users accessing the HCR portion over the Internet are restricted to the data they input into the application. They are restricted from accessing any operating system files on the web server.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?**

Cleared contract personnel are involved in the design and development of this application. Privacy Act information is included in their contracts. All DoS users of consular systems and applications are required to complete the standard computer security training.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

ATS shares data with the Consular Consolidates Database (CCD). All data sharing is for the purposes of completing the processing of the service.

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, Office Consular Systems and Technology, has developed several Internet based business applications. The purpose of these applications is to automate and streamline certain business processes between the Bureau of Consular Affairs (CA), Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), other government agencies, non-governmental organizations (NGOs), and the public. These applications use 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.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**   No.

8) **Who is responsible for assuring proper use of the SHARED data?**

N/A