DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Action Request System- Domestic Operations (ARS-DO) v. 1.0

Conducted by:
Bureau of Administration
Information Sharing and Services
Office of Information Program and Services
Privacy Office
E-mail : pia@state.gov

Privacy Impact Assessment for IT Projects

Introduction

The E-Government Act of 2002 (section 208) imposes new requirements on Government agencies to ensure that system owners and developers consider and evaluate existing statutory and key information management requirements that must be applied to new or modified Government systems that contain personal information.

The purpose of the new requirements* is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government. Section 208 of the E-Government Act requires that agencies now conduct Privacy Impact Assessments (PIA) on all IT projects being planned, developed, implemented, and/or operating regarding individual agency information management systems. The Office of Management and Budget (OMB) has oversight of all federal agency implementation of the Privacy Act of 1974, as amended. OMB will be scrutinizing IT project budget requests based on this new requirement among those already in place. A completed PIA is also required for DOS Information Technology (IT) Security Certification and Accreditation (C&A).

The Office of Information Programs and Services is responsible for the Department-wide implementation of the Privacy Act. This Office will provide assistance in completing the assessment and will present its findings and suggestions in a report for your submission to OMB and/or other appropriate parties.

The goals accomplished in completing a PIA include:

- Providing senior DOS management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;
- Ensuring accountability for privacy issues with system project managers and system owners;
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy; and
- Providing basic documentation on the flow of personal information within DOS systems for use and review by policy and program staff, systems analysts, and security analysts.
- Going through the PIA process will also help to identify sensitive systems so that appropriate information assurance measures are in place, such as secured storage media, secured transmission and access controls.

***** These requirements are drawn from the Privacy Act, Computer Security Act, the Clinger-Cohen Act, the Government Paperwork Reduction Act, the Freedom of Information Act, and Office of Management and Budget (OMB) Circulars A-130: Management of Federal Information Resources and A-123: Management Accountability.

Department of State
Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:
- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/ISS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also please complete the certification page at the end of this document. Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

1) **Who is the Agency Privacy Coordinator who is conducting this assessment?** (Name, organization, and contact information).

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) **Does this system contain any personal information about individuals or *personally identifiable information? If answer is no, please reply via e-mail to the following e-mail address: pia@state.gov . If answer is yes, please complete the survey in its entirety.**

YES _X__ NO___

*The following are examples of personally identifiable information:
- Name of an individual
- Date and place of birth
- Address
- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history

- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

2) What is the purpose of the system/application?

The ARS-DO application is used by the Consular Affairs help desk for domestic information systems and for passport agencies. ARS-DO is a help desk job ticket application that captures the essential information and notes for work requests. These work requests are made for:

- Domestic information system problems which are hardware or application oriented;
- Asset modifications, such as installing or updating hardware or software;
- Network operations, including password requests; and
- Passport issues, such as questions regarding passport applications or problems with issuing particular passports

Although Domestic Operations has used had a previous version of ARS, the one being considered for C&A is a greatly changed one that incorporates many new features, including a COTS help desk module, mid-tier web support, an upgraded web server, and a new host operating system. For this reason, it has been named ARS-DO v. 1.0.

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

The systems under this project were developed and modified to support U.S. immigration and nationality law as defined in the major legislation listed below:

- Immigration and Nationality Act (INA) of 1952 (and amendments);
- Anti-Drug Abuse Act of 1988 (Public Law 100-690);
- Immigration Act of 1990;
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA96);
- Omnibus Consolidated Appropriations Act, 1997 (Public Law 104-208);
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000);
- USA PATRIOT Act of 2001 (HR 3162) (Public Law 107-56); and
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525).

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

1) Does a Privacy Act system of records already exist?

YES _X__ NO__

If yes, please provide the following:

System Name __Passport Records_____ Number ___State-26_____
System Name __Overseas Citizen Services Records___Number ___State-05_

Policies/procedures governing the disclosure of American citizen information is specified various sections of 7 FAM Consular Affairs. The disposition schedule for American citizen records is contained in U.S. Department of State Records Disposition Schedule, Chapter 15: Overseas Citizen Services Records.

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

U.S. citizens seeking or updating their passports are the individuals whose personally identifiable information is captured by ARS-DO.

Department employee work contact information may also be collected; this does not constitute information covered by Department of State privacy practices.

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

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

Individuals provide the primary source of information for their passports. The privacy protected information may be used in the ARS-DO trouble-ticket to either uniquely identify the passport or may itself be the basis of inquiry.

b. Why is the information not being obtained directly from the individual?

N/A

c. What Federal agencies are providing data for use in the system?

N/A

d. What State and/or local agencies are providing data for use in the system?

N/A

e. From what other third party sources will data be collected?

N/A

f. What information will be collected from a State Department employee and the public?

The information is obtained by a DoS passport office employee for reference within the ARS-DO trouble ticket. This information might include the applicant's name, address, passport number, and contact information.

3) Accuracy, Timeliness, and Reliability

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

Applicants provide supporting documentation to corroborate personal information. This might include driver's licenses, utility bills, and the like.

b. How will data be checked for completeness?

The personal information stored on ARS-DO is collected on an ad hoc basis, that is, when suitable for the need. The DoS employee recording the information will collect as much information as is necessary to uniquely identify the passport and/or resolve the passport problem.

c. Is the data current?

The data collected is current to the time and date of the transaction.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

The data is not described in detail within the ARS-DO application. However, there are well-known data standards for U.S. passports.

D. DATA CHARACTERISTICS:

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

Yes, although resolving passport issues is only one of several reasons to use the trouble ticket tracking functions of ARS-DO. Resolving IT asset problems is perhaps the main function for ARS-DO.

2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

No

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

No

4) **Can the system make determinations about employees/public that would not be possible without the new data?**

No

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

N/A

6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

N/A

7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

N/A

8) **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.**

The data is retrieved by trouble ticket number, which is assigned by the system and has an arbitrary connection to the individual applying for a passport.

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

No summary reports based on privacy information can be made by this application.

E. MAINTENANCE AND 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?**

   All clients use the same, normalized database, which is managed by the ARS-DO application.

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

   ARS-DO information consists of help ticket information, which would be considered "IT Customer Service Files," and, therefore, subject to DoS Disposal Authority Number N1-059-02-9, item 10b and 23b. The retention period for this category of data, as outlined by the above disposal authority, is "Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later."

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?**

   Data is destroyed, retired, or archived according to Department of State records disposition schedules.

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

   No

5) **How does the use of this technology affect public/employee privacy?**

   The technologies employed do not affect public privacy.

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   No.

7) **What kinds of information are collected as a function of the monitoring of individuals?**

   N/A

8) **What controls will be used to prevent unauthorized monitoring?**

   N/A

9) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

N/A

10) **Are there forms associated with the system? YES ___ NO __X__**
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)?

F. ACCESS TO DATA:

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

The primary users who access the data are domestic operations support desk personnel and their managers. The application administrator and database administrator may have access to data for the purpose of troubleshooting system and/or database problems.

2) **How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access is determined based on the user's role. User roles are assigned by CA management based on the job the employee will be performing. A request for access is then sent to the ARS-DO application administrator, who then sets up access.

Access criteria and procedures are documented.

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

Users will only have access to the data granted to the role that they have been assigned. Support desk manager can run additional reports, allocate resources, identify trends, and see customer satisfaction information.

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

- Access to data in the system is determined based on the user's role. A user role may allow access to all or only partial data in an applicant record.
- Auditing is enforced at the System, Database and Application levels. All changes to the trouble tickets are recorded.
- All users are required to take DS security training and refresher courses annually.

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?

Contract personnel are involved in the design and development of these systems. Privacy Act information is included in their contracts. All users of CA systems are required to complete the standard computer security training.

6) Do other systems share data or have access to the data in the system? If yes, explain.

No.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

All systems under this program processing passport data are subject to the same processing restrictions regarding access controls, privacy and records disposition.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No.

9) If so, how will the data be used by the other agency?

N/A

10) Who is responsible for assuring proper use of the data?

N/A

ADDITIONAL COMMENTS: *(optional)*