DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

PRM Refugee Processing Center - Worldwide Refugee Admissions Processing System (WRAPS)

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

E-mail: pia@state.gov

The Department of the State
FY 2008 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

Department of State
FY 2008 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.

IT Project Name/Component System: Worldwide Refugee Admissions Processing System (WRAPS)

A. CONTACT INFORMATION:

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

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

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

YES X NO___

**** "Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any**

person not acting in his/her official capacity as a federal government employee/contractor".

If answer is yes, please complete the survey in its entirety.

If answer is no, please complete the certification page and submit the completed PIA to both of the following e-mail address: pia@state.gov.

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

YES X NO _____

If yes, please provide the following:
System Name: SORN-60, Department of State Refugee Processing Center Records

If no, a Privacy system of records description will need to be created for this data.

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

PRM has developed and deployed a standardized computer refugee resettlement case management system. This system, known as the Worldwide Refugee Admissions Processing System (WRAPS), links the worldwide PRM partners with a modernized data communications network capable of facilitating the entire refugee resettlement process. WRAPS tracks refugee applicants as they move through the required refugee processing steps until arrival in the United States.

4) What legal authority authorizes the purchase or development of this system/application? See SORN-60.

C. DATA IN THE SYSTEM:

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

Individuals covered in WRAPS are foreign applicants for refugee status, approved refugees, denied refugees, and those who withdraw from the program**.**

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

a. Who/what is the source of the information?
Refugee applicants are referred to the U.S. Refugee Admissions Program by the United Nations High Commissioner for Refugees, non-governmental organizations and embassies. In some cases, refugee applicants may also apply directly to the program.

b. What type of information is collected from the source of the information?
Biographic information (e.g., name, age, date of birth) nationality, ethnicity, religion, family relationships, persecution claim, etc.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?
SOPs are in place both overseas and domestically for ensuring the accuracy of refugee applicants' records. Each refugee applicant has a face-to-face meeting with a caseworker to verify that the information on his or her record is correct.

b. How will data be checked for completeness?
Quality assurance procedures are in place both overseas and domestically for cross-checking.

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).
WRAPS data is updated on a daily basis overseas and domestically as a refugee moves through the process. Refugee data is updated in WRAPS until 6 months post-U.S. arrival.

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?
Yes

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?
No. Personal data is not derived.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?
No.

4) Will the new data be placed in the individual's record?
No.

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

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.
The data for refugees is retrieved via the WRAPS application using a unique WRAPS Case number, a DHS-provided alien number, or a system GUID.

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 generated….**
The main report produced on individuals is the Refugee Bio-Data Collection. This information is provided to the non-government officials (NGOs) who resettle the cases in the United States. Individual name-check reports are provided to the Department of Homeland Security (DHS) interviewing officers to verify that mandated security checks were performed. Affiliate monitoring reports are produced for PRM/A employees to verify that resettlement services have been provided to arrived refugees.

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?**
Standard Operating Procedures (SOPs) govern worldwide use of WRAPS. The WRAPS software itself also promotes consistency.

2) **What are the retention periods of data in this system?**
Currently, all the data is being retained indefinitely for historical statistical purposes. PRM is working with the Bureau of Administration (A/ISS/IPS-RA) on revising its refugee records retention policies dictating what data will be retained and for how long.

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?**
Currently, all data is being retained indefinitely. Once the refugee retention policy and guidelines have been officially approved by NARA, RPC will develop a data archiving plan in compliance with the new guidelines. Biodata information is passed to the NGOs for their use in resettling refugees. The namecheck reports become part of the refugees' travel packets and end up in DHS alien files. Affiliate monitoring reports become part of the permanent PRM records.

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 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?**
While overseas, address and location information is collected so the applicant can be contacted throughout the approval and departure process. When an individual is resettled in the United States as a refugee, address information may be given and a social security number is supplied by the NGO that resettled the refugee. Access to WRAPS data is limited to specific individuals of specific agencies on "a need-to-know" basis.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**
The Privacy Act System of Records Notice, STATE-60, covers all foreseen uses of the system.

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)?
All official Office of Management and Budget (OMB) approved forms generated by WRAPS contain Privacy Act statements.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system?** (e.g., contractors, users, managers, system administrators, developers, other)
Authorized users include only those who are directly involved in refugee processing under the USRAP. These include U.S. Government employees, contractors, system administrators, and the WRAPS IT team (designers, developers, data engineers, etc.)

2) **What are the criteria for gaining access to the system?** Are criteria, procedures, controls, and responsibilities regarding access documented?
Access to WRAPS data is governed by the Department's PRM's data sharing policy. Each user's access is determined and approved by the systems owner after careful evaluation of the user, their organization, and their need to access WRAPS data.

3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
As explained above, WRAPS data access is determined and approved on a case-by-case basis. Only those users who are directly involved with refugee

processing have access to WRAPS data. User access to WRAPS data is limited by role. Other users have 'Read Only' privileges. They cannot alter any refugee data.

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.)**
Only authorized users involved with refugee processing have access to the WRAPS data. The users are oriented and trained in the Privacy Act as it pertains to use of refugee data. Managers periodically run audit reports to ensure that users are not performing unauthorized functions.

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?**
Yes. Contractors are involved with the design and development of the system and are also involved in the maintenance of the system. The current contract includes Privacy Act clauses; other regulatory measures have been addressed as well. Training and rules of conduct have been established regarding handling of WRAPS data.

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?**
Yes. Memorandums of Understanding (MOUs) are in place between PRM and other entities who receive WRAPS data.

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?**
Yes. DHS officers have access to WRAPS data for refugee adjudication purposes, fraud prevention, and relationship/family tree research related to granting of following-to-join petitions. The Center for Disease Control (CDC) has access to some data for public health purposes and follow-up on arrived refugees. Health and Human Services (HHS)/ORR has access for determining allocation of federal funds to states who provide services to arriving refugees.

8) **Who is responsible for assuring proper use of the SHARED data?**
The data sharing agreement between the Department of State and the Department of Homeland Security (DHS) governs the proper use of WRAPS data. DHS is responsible for ensuring the proper use of WRAPS data by its employees.

ADDITIONAL COMMENTS: *(optional)*

None