DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Waiver Review System v. 03.00.02

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

A. 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 addresses: Frenchka@state.gov; Makaloum@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 WRS subsystem is used by Department of State (DoS) personnel to handle the applications for waivers to 'J' visa requirements. The JWOL and ISCS subsystems are used by exchange visitor visa holders who wish to be exempt from one of the visa requirements. JWOL is used to fill in the application and then print out a hardcopy complete with a barcode. ISCS is used by applicants to track the progress of their waiver requests. Neither JWOL nor ISCS allow users to update any DoS data tables.

This PIA covers WRS system v. 03.00.02, which was, prior to September 2005, three separately named applications: the Waiver Review System (WRS); the Internet Status Check System (ISCS), and the 'J' Visa Online (JWOL). For purposes of clarity, the former WRS will be referred to within this SSP as the WRS subsystem. It was decided to treat these subsystems as one system because they are used for the various steps with a single business purpose: the initiation, handling, and tracking of 'J' visa waiver requests. Accordingly, they will be treated as an integral system for the purpose of this PIA.

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 (P.L. 100-690);
- Immigration Act of 1990;
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA96);
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208;
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000);
- USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56); and
- Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)

C. DATA IN THE SYSTEM:

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

YES _X__ NO___

If yes, please provide the following:
System Name ___Visa Records____ Number ___State-39_____

Policies/procedures governing the disclosure of visa information is specified in 9 FAM 40.4, Furnishing Records and Information from Visa Files for Court Proceedings, and Notes. The disposition schedule for visa records is contained in U.S. Department of State Records Disposition Schedule, Chapter 14: Visa Records.

Policies/procedures governing the disclosure of American citizen information is specified in 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.

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

2) What categories of individuals are covered in the system?
Foreign nationals who are seeking a waiver to their 'J' visa requirement to return from the United States back to their home country. The Exchange Visitor Program, referred to as a J Visa, is carried out under the provisions of the Mutual Educational and Cultural Exchange Act of 1961, as amended. The purpose of the Act is to increase mutual understanding between the people of the United States and the people of other countries by means of educational and cultural exchanges.

For exchange visitors, there is a two-year home-country physical presence or residency requirement. Visitors who are subject to, but do not wish to comply with the requirement, may apply for a 'J' Visa Waiver to remain in the United States beyond the date of their programs. A waiver is also necessary if they seek to submit an application to DHS/CIS for a change in visa status.

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 'J' visa waiver. If the information is not entered on the hard copy form and 3D barcode, then it is obtained from documentation that is submitted with the waiver application by the applicant.

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?

Additional information may be collected by 'J' visa waiver processing personnel from the applicant.

3) Accuracy, Timeliness, and Reliability

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

N/A

b. How will data be checked for completeness?

It is the applicant's responsibility to provide all of the information necessary for the waiver application. Department of State Legal and Waivers personnel will process and check the information for completeness.

c. Is the data current?

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

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

Data is collected on the 'J' visa waiver form, which is available with full instructions from the JWOL website or in hard copy form.

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, the personal data is central to the 'J' visa waiver application process.

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?**
   Decisions on whether to grant the waiver will be entered to the individual applicant's record.

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?**
   Unknown.

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.**
   A case number will be assigned to each application that is paid for and presented to the 'J" Visa Waiver Office. This case number can be used for retrieving case status on the ISCS website (which does not include personally identifiable information) and the WRS subsystem.

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?**
ISCS and JWOL subsystems are updated nightly via an Oracle script. No personally identifiable information is involved in this transfer.

2) **What are the retention periods of data in this system?**
At this time, information is kept indefinitely.

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?**
None are in place at this time.

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?**
N/A

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 DoS Legal Waivers personnel and their managers. The application administrator and database administrator may have access to data for the purpose of troubleshooting the 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 Bureau of Consular Affairs (CA) management based on the job the employee will be performing. A request for access is then sent by the Legal Waivers Office to the Consular Consolidated Database administrators, (CCD), who then set 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 have access only 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 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's 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 Bureau of Diplomatic cyber-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 the 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?**
   N/A.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**
   Yes, the Department of Homeland Security (DHS) will access this data.

9) **If so, how will the data be used by the other agency?**
   Data will be used to make a decision to grant a waiver.

10) **Who is responsible for assuring proper use of the data?**
    DHS's Privacy Office puts into place controls to assure the proper use of the data.