DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Electronic Diversity Visa (EDV) System

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)
Email : pia@state.gov

Department of State
Privacy Impact Assessment

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: 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?

EDV data is a mission-supportive system that supports the mission of the Diversity Visa Lottery Program with an electronic application-capture process based on Web technology and the Internet. EDV reduces costly data entry errors and provides a better method for preventing duplicate applications.

The applicant information consists of name, address, country of birth, country of eligibility, and a digital photo of the applicant. Applicants are not U.S. citizens, therefore, the information obtained is not protected under the Privacy Act. However, the information shall be considered sensitive, by the Immigration and Naturalization Act of 1952, and codified in United State Code Title 8, Chapter 12, Subchapter II, Part III, Section 1202 (f):

> Confidential nature of records: The records of the Department of State and of diplomatic and consular offices of the United States pertaining to the issuance or refusal of visas or permits to enter the United States shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States…

Potential applicants from all over the world can access the application by visiting the URL http://dvlottery.state.gov or http://travel.state.gov/dv2006.html during the 60-day registration period.

There are three distinct phases of EDV's operation:
1) During Phase I, the EDV system resides at an Internet Service Provider (ISP) in Ashburn. The ISP, through a Service Level Agreement (SLA), provides the facility, network environment support, and bandwidth capacity.

2) During Phase II, the prepared data in Ashburn becomes available to the Kentucky Consular Center (KCC) users through a secure socket layer (SSL) connections. The KCC local area network (LAN) does connect to OpenNet.

3) During Phase III, a copy of the EDV Database is transferred to KCC for the purpose of data mining to support CA/VO and the visa adjudication process.

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

The Immigration and Nationality Act (INA) established a program in 1995 whereby an annual numerical limitation of 55,000 Immigrant Visas would be awarded each year to natives of specific "low admission" countries through a process knows as the Diversity Visa (DV) Lottery Program.

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 _39___

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?
Individuals who have applied for visas.

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?

The individual or a service the individual chooses to use in order to input their information in the system. These services are not in anyway connected to the EDV system or project.

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

For convenience, an individual can have their personal information entered by a service.

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

No federal agencies are providing data.

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

None.

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

None.

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

None. The individual or a service of his or her choosing will directly provide all collected information.

4) **Accuracy, Timeliness, and Reliability**

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

N/A based on answers from section 3 above.

b. How will data be checked for completeness?

Required fields must contain an entry for the form to be accepted. The application fields within the web page handle the validation controls of submitted information by limiting the type information that can be entered,

such as alpha or numeric, or by providing drop down pick lists of available information choices.

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).

Information can only be submitted during a 60-day enrollment period and afterwards becomes the system of record for that year's lottery. Each year's lottery has its own enrollment period. Applications from previous lotteries are not carried forward to the next year's lottery. If an individual is not selected as a winner for a current year's lottery the applicant may submit a new application when Phase 1 for the next year begins.

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

The data elements are described in System Security Plan, Detailed Design Document and the System Requirements Specifications.

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.

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?

N/A based on response to #2.

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

Yes.

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

N/A based on response to #2.

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

Controls that are in place to protect the data from unauthorized access or use are Authentication and Access Control Lists (ACLs). Authentication for the EDV system, users in the groups System Administrators, Database Administrators, Web Administrators, Network Administrators, KCC Users, and ISSO users will provide a password. Password management is handled in accordance with the policy in 12 FAM 623.3-1. Once authenticated, ACLs, are lists associated with a file or a resource that contains information about which users or groups have permission to access a resource. The EDV system employs logical access controls in accordance with the principle of least privilege and the concept of separation of duties.

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

Yes, the proper controls are remaining in place to protect the data and prevent unauthorized access. The controls that are currently in place secure the data from intrusion and compromise.

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 indexed by a Lottery Rank Number (LRN) by which the users at KCC are able to retrieve the data.

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

Reports that will be produced on individuals vary from photo and work packages completed. The use of the report identifies the progress as to where a LRN is located. The reports that are produced by the system are only accessible by users who have access to the system. See answer to question 8

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?

The system is operated in more than one site but consistent use of the system and data is not required at both sites. The database from the previous year's lottery is transferred to KCC after lottery winners are selected. A new database is

established in Ashburn for the following year's lottery in order to receive subsequent application submissions.

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

Retention periods are not yet defined and are being developed in cooperation with A/ISS/IPS/PP/LC.

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?

Disposition procedures are not yet defined and are being developed in cooperation with A/ISS/IPS/PP/LC.

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 based on response to #4.

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

The system provides the capability to identify and locate individuals, but not monitor individuals. Applicants submit applications in the hopes of being selected to obtain an immigrant visa, and, therefore, must submit accurate information on how to be contacted in the event of being selected.

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

N/A based on response to #6.

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

N/A based on response to #6.

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

No.

11) 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)?

No.

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 following will have access to the data: database administrators, developers, and system administrators.

There are three types of KCC users: (1) Super Users; (2)Team Lead Users; and (3) Users.

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

Users receive access through local requesting procedures inherent to the CA organization and are compliant with 12 FAM policies. Each user must submit an account request form indicating the requirement for privileges to the system (Super User, Team Lead or Regular User). The account request is reviewed by the user's supervisor and must be approved by an EDV Super User before the request can be granted. Users are setup via Super User located at KCC because they are the process owners for the EDV system.

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

User access will be limited depending upon job function. Database administrators and developers will have the most direct access to the data. System administrators will have indirect access to the data since they are responsible for performing backups.

The three types of KCC users have the following access. Super Users are authorized to create, edit, disable, and activate additional users; download batch files; and create reports. Team Lead Users are authorized to run reports; configure user assignments; adjust thresholds; review packages; and process packages. Users are authorized to view and process packages.

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)

There are three levels of controls in place to minimize the unauthorized browsing of data by those having access. First, all users of the system are required to complete Computer Security Awareness Training, at which time they sign a Rules of Behavior statement acknowledging appropriate use of DoS computers. Second, access controls are applied depending upon the assigned role of the user that allows access based upon the "need to know." Lastly, auditing is enabled to record access based upon unique identification assigned to each user.

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, development, and maintenance of the system. A limited background investigation is the responsibility of the Bureau of Diplomatic Security (DS), in conjunction with normal hiring practices. The background investigation consists of a review of a completed security questionnaire, a name check against applicable U.S. Government, police, credit and fingerprint records, and may include a personal interview if warranted.

Only cleared technical personnel (U.S. Government and contractors) are allowed to access the computer rooms housing EDV servers, and no one is allowed to access the system until a limited background investigation has been completed. In addition, all domestic Bureau of Consular Affairs positions are reviewed for sensitivity level.

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 based on response to #6.

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 based on response to #8.

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

N/A based on response to #8.