DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Diversity Visa Information System
(DVIS)
Updated April 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Email : 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 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 Diversity Visa Information System (DVIS) is used by the Kentucky Consular Center (KCC) to process more than 6 million applications received each year for the Diversity Lottery. The system provides the users with the capabilities to record beneficiary data; record duplicate and other fraudulent applications; allocate cases based on cut-off numbers received from the Visa Office; and to transmit data to the Immigrant Visa Overseas (IVO) systems at posts for final processing.

When the application period is over, a program is run to randomly pick the winning entries.

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 (Pub. L. 100-690);
- Immigration Act of 1990;
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (IIRIRA96);
- Omnibus Consolidated Appropriations Act, 1997 (Pub.L. 104-208);
- Legal Immigration Family Equity "LIFE" Act (Part of HR 5548, 2000);
- USA PATRIOT Act of 2001 (HR 3162) (Pub. 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 Record_____ Contract Number State-39
Policies/procedures governing the disclosure of visa information are stated 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 are 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?
Non-U.S citizen visa applicants are the primary individuals covered by DVIS.

Department of State employee and contract employee information, such as names, are collected and stored with the applicant's record as it relates to the auditing of actions taken during the processing of a visa application.

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.

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?
The Federal Bureau of Investigation is the only federal agency that provides data to be used by this system under this program.

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?
Information collected from DoS employees includes data relevant to the auditing of the visa adjudication process, such as employees' names.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?
Data provided to the Department is manually reviewed by contract staff or Department personnel for accuracy prior to being input into DVIS

b. How will data be checked for completeness?
This will be accomplished through the same process as described in 3a above.

c. Is the data current?

The data collected is relevant to a visa applicant who may apply one or more times. If the data is considered to have a derogatory impact on the issuance of a visa to the applicant, the information is retained in a case file. The data is re-examined for validity and relevance to each visa application.

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

The data elements for this system are described in its Data Dictionary.

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

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

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?**
Access to all system data is controlled through the use of user roles in the DVIS Primary Oracle Server (POS).

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.**
Data is routinely retrieved using name, date of birth, and place of birth. Depending on the system used to process the applicants' record, case numbers or applicant IDs can also be used to retrieve applicant 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?**
The systems covered under this program produce a wide variety of reports. Those reports specific to individuals are visa case reports, which list the details of a specific visa case. Such reports are used to review and document the details of a specific visa case. Only authorized users, based on users' roles, would have access to these reports.

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?**
CA employs configuration management controls over the software used to process applicant data. Databases that contain visa applicant data are under strict control of the CSD Data Engineering Team who insure data integrity and data base reliability.

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

Visa applications are retained for the length of the visa validity period plus one year. This is in compliance with the Visa Lookout Accountability provisions of the Illegal Immigration Reform and Immigration Responsibility Act of 1996. The complete disposition schedule for visa records is specified in the U.S. Department of State Records Disposition Schedule, Chapter 14: Visa 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 visa records is specified in the U.S. Department of State Records Disposition Schedule, Chapter 14: Visa 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?**
N/A

6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
The system under this program can be used to identify individuals through the use of basic biographic information. The systems can also be used to monitor employee activity as it relates to the auditing of the visa adjudication process. DVIS is **not** used to locate individuals.

7) **What kinds of information are collected as a function of the monitoring of individuals?**
Auditing data, such as employees' name, are collected for the purposes of auditing the visa application and adjudication process. Access to audit reports is limited to management personnel.

8) **What controls will be used to prevent unauthorized monitoring?**
Audit reports are available only to system administrators and CA management personnel.

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 consular managers and contractors in the roles of analysts, data-entry clerks, and systems administrators. Developers may also 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 users' roles. Users' roles are assigned by the Bureau of Consular Affairs (CA) management based on the job the employee will be performing. Only system administrators are allowed to create user roles.

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 record. Auditing is enforced at the system, database and application levels. All users are required to take the Bureau of Diplomatic Security (DS) 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 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.**

System data is stored in the Consular Consolidated Database (CCD) from which other CA systems can access the data if assigned the proper role.

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 visa 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)?

Yes. Other federal agencies involved in Border Security share data and have access to CCD-VOIS data, but will not interface directly with the system.

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

Other agencies use data provided by these systems for border security and law enforcement purposes. A memorandum of understanding (MOU) is usually implemented between the data owner, the Visa Office (CA/VO), and the agency receiving the data to define how the data will be used.

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

The recipient of the data is responsible for assuring proper use of the data as defined in the applicable MOU.