DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Visa Opinion Information Service (VOIS)
PIA COMPLETION DATE: January 9, 2008

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

A. 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: _Visa Records_____ Number: _State-39___

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?

The Visa Opinion Information Service (VOIS) provides a graphical user interface (GUI) to the Consular Consolidated Database (CCD). It acts as a toolkit to simplify the access, the management, and the analysis of the data available in the CCD. It supports the Visa Office (VO) business process of rendering Security Advisory Opinions (SAOs) and Advisory Opinions (AOs). VOIS is a WebForms/ASP.NET implementation that allows for convenient, extensive integration with the data and hypertext markup language (HTML) reports available within the CCD. No data is stored directly in VOIS; it is strictly an interface to CCD data. VOIS also allows users to submit name check requests to the CLASS system and requests for clearances from outside information agencies.

The service main manipulation is to tracks all actions surrounding an SAO/AO from the point the record is received in VOIS to the point when it is completed and archived. All user actions on the SAO/AO are audited at the database level. All service actions on an SAO/AO, such as updates from the CCD, are captured and tracked. When a user sends a response to a SAO/AO request, the text of the response will be stored in the CCD and will be available for viewing. Multiple VOIS users can view the same VOIS document simultaneously.

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

8 U.S.C. 1101-1503 (Immigration and Nationality Act of 1952, as amended).

B. DATA IN THE SYSTEM:

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

Non-U.S citizen visa applicants are the primary individuals covered by VOIS.

Department 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.

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

a. Who/what is the source of the information?

The primary sources of information are from the DVIS, IV, and NIV systems that manage the visa application process. These systems obtain their information from the individual visa applicant and/or petitioner. Some information is acquired from other agencies and also developed by Visa Office staff.

Other federal agencies that provide data used by this system include:

- Department of Homeland Security;
- Federal Bureau of Investigation;
- Entities within the Intelligence Community; and
- Drug Enforcement Administration.

Some data is collected on behalf of the Department of State by third party service providers, such as banks, travel agents, appointment schedulers, etc. under contract with the Department (domestic) or overseas posts.

b. What type of information is collected from the source of the information?

Information collected from the sources includes data relevant to the individual visa applicant and auditing of the visa adjudication process, such as full name, home address, social security number, date of birth, place of birth, phone number, email address, and other information related to the applicant.

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 by other agencies and service providers are verified by contract staff or FSNs during routine visa application processing and by a DoS consular officer at the time of visa adjudication.

Data provided from the visa applicant is also verified during the adjudication process.

b. How will data be checked for completeness?

This will be accomplished through the same process as described in 3.a above.

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).

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 and will be purged on their 90th birthday. The data is reexamined for validity and relevance to each visa application when the applicant re-applies for a visa.

C. 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, the data used by VOIS is both relevant and necessary for the purpose of collecting, processing, and storing personally identifiable information used to process visa applications.

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, the data collected will not be derived or aggregated. As part of the CCD, VOIS is a Sensitive But Unclassified (SBU) service, and, therefore, classified material is restricted from being scanned into or stored in the CCD via VOIS. A standard warming message regarding to SBU guideline is displayed when users authenticate to the CCD. VOIS provides the capability for users to note that additional classified information outside the automated service is available on an

applicant/SAO/AO, without divulging any classified data. This capability can be used to indicate an external source of information that may be classified. VOIS provides the file room with the utilities and reports to continue to manage these files manually.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

N/A; no new data is created.

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

N/A; no new data is created.

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

N/A; no new data is created.

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.

Data is routinely retrieved using name, date of birth, place of birth, case numbers or applicant IDs to retrieve an applicant's data.

7) 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 would be visa case reports, which list the details of a specific visa case. Such reports would be used to review and document the details of a specific visa case. Only authorized users, based on the user's role such as Visa Office – Information System Liaison (VO/I), Legal Coordinators (LC), Legal Advisor (LA), and Public Inquiry (P/I) would have access to these reports.

D. 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?

The Bureau of Consular Affairs (CA) employs configuration management controls over the software that is used to process applicant data. Databases that contain visa applicant data are under strict control of the CSD Data Engineering team who ensure data integrity and database reliability.

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

If a case file is created for a visa applicant, it is retained till his/her 90th birthday. If the information developed is not considered to be derogatory and/or relevant to the applicant and the visa application, then the case file is deleted; though the unclassified report generated by VOIS will be retained by the Visa application system through which the applicant applied and kept for the life of that record.

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, VOIS does not uses technologies in ways the Department has not previously employed.

5) How does the use of this technology affect public/employee privacy and does it restrict access to the system?

Access to VOIS is restricted to clear DoS authorized users such as VO/I, LC, LA, and P/I. All information collected by VOIS is voluntary provided by visa applicants and is used solely to process visa application and visa adjudication.

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?

VOIS is not used to locate individuals. VOIS can be used to identify individuals through the use of basic biographic information or using biometric information such as photos and/or fingerprints and they can also be used to monitor employee activity as it relates to the auditing of the visa adjudication process.

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

No, the system functionalities might be modified but the content of the information is still the same.

8) 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)?

E. 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 Visa Office – Information System Liaison (VO/I); Legal Coordinators (LC); Legal Advisor (LA) and Public Inquiry (P/I); Foreign Service Officers (only see the end products produced by LC); other full time employees; consular managers; contractors in the roles of analysts; data-entry clerks; visa adjudicators; and systems administrators. At some facilities, contractors fill the role of data entry clerks. Developers may have access to data for the purpose of troubleshooting system and/or database problems.

2) **What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?**

Access is determined based on the user's role. User roles are assigned by the CCD Certifying Authority or post administrator based on the job the employee will be performing. Only CCD system administrators are allowed to create users and assign user roles.

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.

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.)**

Access to data in the systems under this program 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. A subset of the access to records is audited. Audit trails are used to document the actions taken in processing a particular request for service, particularly adjudication and printing of a travel document. In addition, all users are required to attend a DS security briefing, usually on an annual basis.

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 and pass the standard computer Cyber security training.

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

The recipient of the data is responsible for protecting the privacy rights of the public and employees affected as defined in the applicable Memorandum of Understanding (MOU). A MOU is usually implemented between the data owner, the Visa Office, and the agency receiving the data to define how the data will be used and protected.

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. Other federal agencies involved in Border Security share data and have access to VOIS data by connecting to the CCD system directly through the Interlink-U portal via the DoS Extranet. The data is used to assist consular officers in the Department and overseas in dealing with problems of a legal, technical or procedural nature that may arise in considering an application for a U.S. visa.

8) **Who is responsible for assuring proper use of the SHARED data?**

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