DEPARTMENT OF STATE
PRIVACY IMPACT ASSESSMENT
ECA Program Management and Outreach System (ECA-PMOS)
Updated June 2008

A. CONTACT INFORMATION:

Who is the Agency Privacy Coordinator who is conducting this assessment (Name, organization, and contact information)?

Ms. Margaret Grafeld, Director
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

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**___

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

YES X NO____

If yes, please provide the following:
System Name: Education and Cultural Exchange Program Records

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

The system supports the mission of the Bureau of Education and Cultural Affairs (ECA) to collect and maintain information on participants in the Bureau's many exchange programs and provide outreach to the participants and the public.

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

The Federal Records Management Acts (Pub. L. 81-754, Pub. L. 94-575), the Smith-Mundt Act (Pub. L. 80-402) and the Fulbright-Hayes Act (Pub. L. 87-256).

C. DATA IN THE SYSTEM:

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

American and foreign national participants in ECA exchange programs as well as American host families.

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

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

The sources of information are individuals, including both Americans and foreigner nationals participating in exchange programs, either directly or from information already collected *by* or *for* the Department via

- Public Diplomacy staff at an embassy, after prior collection from the individuals.
- Non-government officials (NGOs) acting under grant to the Department of State (DoS).
- Individuals who enter information directly into a paper form or a form on a Department web site.
- One component information systems to another component information system (for use related to the original reason for the data collection).

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

Name, date of birth, place of birth, social security number, gender, address, phone number, email address, passport information, visa type, medical information, insurance card number, marital status, information about occupation, spoken languages, and financial information.

3) Accuracy, Timeliness, and Reliability

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

All information is collected by post staff, ECA staff, Grantee Organization staff, or the individuals can enter their own information directly onto forms. When possible, information is verified by the individual at the time of collection.

b. How will data be checked for completeness?

There are business rules to validate information completeness. Each sub-system enforces its own business rules defining the required data fields before a record can be created. This includes ensuring the values for all required fields are of the correct type and/or in a defined range. When possible, lookup tables and list box controls are used to limit data errors. Records failing to meet these requirements cannot be created or saved.

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).

Yes**.** In order to maintain data accuracy, all parties involved in information collection have multiple check points. All information collected is date/time

stamped for auditing purposes. Data processing business rules are outlined in each system's technical documentation and user guides. Where sub-systems require users to input personal data (e.g. in registration), users can update their own data and are responsible for such updates. Users of each component application follow their organization's business rules for ensuring information is up-to-date.

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. The PII collected is necessary for:

- Verifying individuals' identities (e.g. primarily SSNs for US citizen participants);
- Approving candidates for Department of State educational and cultural exchanges;
- Department of Homeland Security issuing form DS-2019, which is required prior to issuance of a category J visa for an exchanges participant (US citizens do not complete form DS-2019s); or
- Contacting participants, the staff schools, and other non-profit partner organizations.

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?

The ECA-PMOS does not create new data by linking or aggregating PII from different sources.

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

Not applicable. This system does not create new data.

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

Not applicable. There is no new data to place in a person's record.

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

Not applicable. Per answers to questions D2 through DA4 above, there is no new data.

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.

Although an individual's name can be used to retrieve their personal data, data can also be retrieved by searching other data fields. The more popular methods include the name

and project number of the exchange program; country; participation date; organization/division/branch responsible for the project; program officer's name; and fiscal year.

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 on individuals include lists of project or program participants, contact lists, biographical data, and program booklets. Most reports are used by Department managers and staff in the management of an exchange program to introduce exchange participants to organizations and individuals with whom they will interact during their exchange program (detailed PII data is not shared in these instances); to fulfill requirements of high schools, colleges and universities where they will enroll; to allow Department staff to contact current exchange participants and alumni of exchange programs; and to fulfill requirements of the Department of Homeland Security (DHS).

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?

Information consistency is maintained using data replication and nightly export/import processing.

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

ECA-PMOS data is archived locally after five years but can be accessed when specific search criteria is entered. ECA is currently working with the Department's Records' Officer to create records disposition schedules for the data.

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?

Records will be destroyed or archived in accordance with the system's disposition schedule and personal information is maintained as required by National Archives and Records Administration (NARA). Only authorized personnel have access to permanent records to prevent unauthorized use and inaccuracies.

4) Is the system using technologies in ways that the DoS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

No. The ECA-PMOS uses standard user ID and password authentication to restrict access to only approved users of each sub-system containing PII. Login is monitored and an audit trail records user session information, both of which are standard uses of these technologies. The system uses the Department's network infrastructure to operate the system according to its intended use.

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

Not applicable.

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

ECA-PMOS is not being modified; however, the system was renamed to more accurately represent the types of subsystems that comprise ECA-PMOS. The former system, Exchange Database System (EDS) was renamed ECA-PMOS, before EDS was retired with some of its child systems. The remaining active child systems are now child systems of ECA-PMOS.

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)?

The State Alumni website registration form is designed specifically for use with ECA-PMOS. The Alumni Archive is an intranet web application available via OpenNet only. Access to update data is limited to authorized Department employees, who are required to submit only the data needed to authorize their access and determine what permissions they should have consistent with a "need to know." These users are acting in their official capacity, not as members of the public. The Alumni Archive refers users to the Department's Intranet Privacy Policy.

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

For most of the ECA-PMOS subsystems, access is via OpenNet only and is limited to Department government employees, contractors filling the equivalent DoS staff roles, and IT staff (analysts, developers, database administrators, testers, system administrators, etc), some of whom are contractors.

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

Procedures for access to OpenNet are documented by the Bureau of Information Resource Management. Criteria, procedures, controls and responsibilities for access to each ECA-PMOS sub-system are documented in the system documentation.

Access is granted based on a "specific need to know" depending upon the user's job role, from which a "need to know" can be explicitly inferred. When it is determined that an individual has a need for access to a specific sub-system, they are approved by the system owner for specific roles/access to the sub-system and then granted access and assigned either a user role (a set of permissions) or a customized set of permissions, based on the access they need in order to perform their job.

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

   Access is restricted by application (sub-system) and role, both of which are based on a "need-to-know."

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)**

   Application controls are implemented within the database and application to ensure that unauthorized attempts to modify data do not occur. Application controls are designed into the user interface based on business processes and business rules specified by the application owner. These controls are then linked to the data through database roles and privileges and data validation requirements. Application controls for each sub-system limit not only access to records but also limit user privileges for creating, reading, updating, and/or deleting records to only those records for which they need these privileges. Audit trails record when users are logged in, which tables they access, and how the tables are accessed (read, write, update, delete).

   Training classes, training manuals and training videos are provided to ensure the application is being used in the appropriate manner. All application users must take and pass online security training before they have access to any application.

   Privacy Act clauses are included in the contracts for the contractors who design, develop and maintain the various ECA-PMOS sub-systems. Additionally, rules of conduct have been established and training is required.

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 ECA-PMOS. Privacy Act clauses are included in their contracts. Rules of conduct have been established and training is required.

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?**

   No.

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?

The Department of Homeland Security (DHS) requires electronic submission of specific data before it issues Form DS-2019 which is required before consular officers can grant a 'J' Visa to a DoS exchanges participant. This data is provided to DHS/USCIS by the ECA-PMOS system via a DHS secure website. DHS uses the data to track participants from foreign countries to their entry point into the United States.

Information on awards for Institutional Grants is transferred to the Department's Global Financial Management System (GFMS) to create an official payment obligation. GFMS transfers the data to the Department of Education's Payment Management System (PMS) to allow PMS to pay the grantees. Reversing this process converts the transaction into data.

Information on Institutional Grants awarded is transferred to the Department's Grants Data Management System (GDMS). GDMS transfers the data to the General Services Administration (GSA) for posting to the USA Spending Website, thereby complying with the Federal Financial Accountability and Transparency Act (FFATA) and the Census Bureau's Federal Assistance and Award Data System.

Grant solicitations are posted to the Grants.Gov website, where grant proposals can be electronically downloaded.

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

The Department of Homeland Security (DHS) is responsible for assuring the proper use of the data that is shared with them. The Department's Bureau of Administration is responsible for assuring proper use of the shared data with USA Spending and FAADS. The Bureau of Resource Management is responsible for assuring the proper use of the shared data with PMS. ECA must comply with shared usage and security and safeguarding policies established by Grants.Gov.