Department of State
Privacy Impact Assessment
International Information Program - Program Management and Outreach System (IIP-PMOS)
Updated June 2008

A. CONTACT INFORMATION

Who is the Agency Privacy Coordinator who is conducting this assessment?

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 (PII) about individual members of the public**?**

YES X **NO**___

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

If yes, please provide the following:
System Name: Speaker/Specialist Program

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

IIP-PMOS consists of custom developed applications that support the mission of the Bureau of International Information Programs (IIP). IIP-PMOS acts as a central repository to track the funding, authorization, solicitation, significant communications, and evaluation for many projects, including but not limited to:

- Speakers;
- Electronic Telepress Conferences;
- Digital Video Conferences;
- DVC/Webchats; and
- Webchats.

The Distribution and Records System (DRS) contains the names, interests, and current contact data (addresses, phones, etc) for all target audience "members" (derived from a mission-wide analysis of indigenous influence patterns), as well as information concerning actual contacts with these audiences. Contact with audiences can be via outreach and library programs, attendance at speaker programs, personal contact, receipt of State Department magazines, etc.

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

The Federal Records Management Acts (Pub. L. 81-754 and 94-575) and the Smith-Mundt Act.

C. DATA IN THE SYSTEM:

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

Private citizens and U.S. Government personnel/contractors.

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

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

Information comes directly from the individual.

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

Sub-system	Data Field
DRS	• Name (in a single field for purposes of alphabetic sorting; e.g. "Smith, John") • Mailing Name 1 (e.g. "Mr. John Smith") • Mailing Name 2 (e.g. Mr. and Mrs. John Smith") • Name of spouse • Title • Sub-Title (actual role; e.g. foreign affairs editor) • Protocol (how important *is* the person?) • Responsible officer(s) (U.S. Mission personnel responsible for interacting with the person) • Region (location of the person within the country; e.g., a province) • Physical address (street, city, postal code, whether office or home, which to use for mailings)

Sub-system	Data Field
	• Communication address (e.g., land line, cell phone, pager, fax, internet address, home page) • Occupation • Institution affiliated with • Interests • Mailing list(s) to which the person belongs • Exchange program(s) (name of program and year of participation) • Language(s) (name of language and speaking/writing proficiency) • "Events" involving the person • Comments (about the person)
Tracker	• Name of individual (Last, First, Middle) • Current home and work addresses • Passport Number, type and issue information • Appropriate visas for the subject travel • Telephone numbers (home, work, cell, emergency contact phone number) • Social Security Number • Education • Employment

3) Accuracy, Timeliness, and Reliability

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

All data is collected from individuals by IIP staff and entered manually through the application.

b. How will data be checked for completeness?

Business rules are in place to validate data completeness. Program officers and coordinators manually verify that the data is complete and accurate. Grants and vouchers will not be authorized if required data is missing. These documents are generated directly from system.

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**.** All parties involved in data collection have multiple check points to maintain data accuracy. Program officers verify with the grantees that their personal data and bios are updated and accurate. All data collected is date/time stamped for auditing purposes.

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 information is collected because it is necessary for:

- Verifying individuals' identities;
- Approving candidates for the Department's Speaker Program;
- Generating federal assistance awards (Form DS-1909) and public vouchers (Form SF-1034A);
- Managing and tracking post and IIP budgets;
- Obtaining proper visas and travel itineraries; and
- Mapping programs to DOS goals and objectives.

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 IIP-PMOS does not create new data by linking or aggregating PII from different sources. All PII data is maintained on secure databases and servers that have been certified and accredited.

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. There is no new data.

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

Not applicable. There is no new data to place in an individual's record.

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

Not applicable. There is no new data that is derived or aggregated.

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 retrieved by an individual's name. However, searches can also be run on home and business addresses, travel itinerary, social security numbers and passport number.

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

Financial reports for grants and travel reimbursements are produced as well as emergency contact information for speakers in the field. Grants and travel reimbursement forms authorize financial transactions and provide an audit trail. Reports for speakers in the field provide emergency contact information for duty officers. Only authorized Department of State employees have access to the reports.

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?**

Not applicable. The IIP-PMOS operates at one site only.

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

The Bureau of IIP is currently working with the Department's records managers to create a Records Disposition Schedule for IIP-PMOS.

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?**

Once this system has an approved schedule, records will be destroyed in accordance with the National Archives and Records Administration (NARA); and personal information will not be maintained any longer than required.

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

No. IIP-PMOS uses technologies that the Department has previously employed, on a network infrastructure and 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. The technology has been employed by DOS previously. The system is restricted to authorized OpenNet users only**.** For Active Directory uses a network ID to map to an account to an access system and does not collect additional information that would impact privacy.

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

Not applicable. IIP-PMOS is not being modified. All systems are in the operations and maintenance phase.

7) **Are there forms associated with the system?**

There are no forms used to collect the information in this system. Authorized program officers input data from the individuals via interviews.

F. ACCESS TO DATA:

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

Authorized OpenNet users and technical support have access to the data. Individual grantees have no direct access to the system data.

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

The primary functional administrator determines, on a case-by-case basis, those individuals who can access the system. Factors used to determine access are the individual's assignments and responsibilities. Procedures involving access are documented in project documentation as well as network documentation.

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

Users' access is restricted based upon a user's need-to-know role.

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)

Annual, recurring security training is conducted by the Bureau of Diplomatic Security (DS). Server audit trails contain a record of system activity and user activity including invalid logon attempts and access to data. Access to server audit logs is granted on a "need to know" basis.

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

Application controls for each sub-system limit access to records and user privileges for creating, reading, updating, printing and/or deleting records

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 various IIP-PMOS sub-systems. Privacy Act clauses are included in all contractors' contracts. Rules of conduct have also 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?**

No.

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

The system manager/owner is responsible for assuring proper use of the data.