DEPARTMENT OF STATE

FISCAL YEAR 2008

PRIVACY IMPACT ASSESSMENT

Speakers Program Database Tracker
(TRKR)
[Sub-system of the IIP Program Management
and Outreach System, IIP-PMOS]

Conducted by:
Bureau of Administration
Information and Sharing Services
Office of Information Programs and Services
Privacy Office
E-mail: pia@state.gov

The Department of the State
FY 2008 Privacy Impact Assessment for IT Projects

Introduction

Section 208 of the E-Government Act requires that agencies now conduct a Privacy Impact Assessment (PIA) for all new and significantly modified Information Technology (IT) projects. This includes projects that are requesting funding from the Office of Management and Budget (OMB), non-major systems requesting funding internally and those undergoing DOS IT Security Certification and Accreditation (C&A) process. The Privacy Impact Assessment (PIA) is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system;
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

The PIA will help DOS employees consider and evaluate whether existing statutory requirements and key information management concepts are being applied to new and modified systems that contain personally information about members of the public. OMB, which has oversight of all federal agency implementation of the Privacy Act of 1974, as amended, will be particularly scrutinizing IT project budget requests on the Exhibit 300 based on the PIA in addition to the other requirements that are already in place. The score obtained on the PIA among other criteria will determine the funding of the IT project. IT projects scoring poorly on the PIA will be at risk of not being funded by OMB. The same scrutiny will be applied to non-major funding requests as well as systems undergoing the C&A process. Consequently, it is imperative that the attached PIA be fully **completed, certified and submitted** as indicated below.

The Office of Information Programs and Services (IPS) is responsible for conducting the PIA as part of its Department-wide implementation of the Privacy Act. The PIA will be reviewed and scored by IPS and will be provided with the Exhibit 300 to OMB. This score will reflect how well your system protects personal information and will be integrated with the score for security. This combined score will then be incorporated in your Exhibit 300 submission to OMB. The document will also be provided to the Office of Information Assurance for purposes of C&A. For non-majors, IPS will retain PIAs on file for future needs. A guide and a handbook are being provided along with the PIA questionnaire. Please refer to the PIA handbook while completing the questionnaire. For more detailed information you may refer to the guide. In addition, this Office will assist you in completing the PIA questionnaire should you have any questions not covered in the guide.

Department of State
2008 Privacy Impact Assessment

Once completed copies of the PIA may be provided to the following:

- Bureau/office IT Security Manager (when a C&A is required);
- Office of Information Programs and Services (A/ISS/IPS) Privacy Act Program Staff must be provided a copy of the PIA in all cases;
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Please note that you will receive a low score if all appropriate questions are not adequately answered and/or if the certification page is not completed fully. A guide and handbook are provided along with the PIA questionnaire. **You must refer to the handbook as you complete the PIA. The handbook mirrors each section of the PIA and provides instructions for each question.** For more detailed information, please refer to the guide.

A. CONTACT INFORMATION:

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

Ms. Charlene Thomas
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)

B. 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?

The SPD (Tracker) system acts as a central repository for the Bureau of International Information Programs (IIP). It tracks the funding, authorization, solicitation, significant communications, and evaluation for many projects, including but not limited to:

- Speakers;
- Electronic Telepress Conferences (TPCs);
- Digital Video Conferences (DVCs);
- DVC/Webchats; and
- Webchats.

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

The Federal Records Management Acts (Public Law 81-754, Public Law 94-575).

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: **Speaker/Specialist Program Records** **Number: State 65**

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?

Government personnel, contractors, and private citizens.

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 information comes directly from the individual.

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

Not applicable. See "C3a" immediately above.

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

None.

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?**

The Department's Bureau of Consular Affairs Visa and Passport Offices for visa requirements and the Office of Personnel Management (OPM) provides per diem and travel rates.

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

See "C3e" immediately above.

3) **Accuracy, Timeliness, and Reliability**

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

Interviews with subject individuals.

b. **How will data be checked for completeness?**

Verification against subject individual's driver's license or passport.

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).**

Verification with subject individual on recurring basis.

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

Not applicable.

D. <u>DATA CHARACTERISTICS:</u>

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?**

   Not applicable.

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

   No**.**

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

   Not applicable.

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

   Not applicable.

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

   Not applicable.

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 retrieved from a U.S. Department of State application and data files.

9) **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. Authorized U.S. Department of State employees have access to the reports.

E. <u>MAINTENANCE AND ADMINISTRATIVE CONTROLS:</u>

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.

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

.

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?**

Procedures for disposition of data at end of retention period are not applicable as their retention is indefinite.

Any paper copies of reports will be retained internally by Department of State officers until the copies are no longer needed and then will be destroyed appropriately. See A-02-066-09 Reference File

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?**

Not applicable.

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

Yes, but only when performing U.S. Department of State sanctioned duties.

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

Travel itineraries and grant utilization are collected.

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

Access is available only to authorized DoS employees performing sanctioned duties.

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

Not applicable.

10) **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)?

The access to the system is granted after the requestor of the access, grant, or travel signs the request form acknowledging reading and understanding the Privacy Act statement.

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 users and technical support staff have access to the data.

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

   The primary functional administrator determines access to the data on a case-by-case basis.

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

   Users are restricted by role.

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)**

   Users must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through Diplomatic Security.

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 follow all criteria in number F4 above.

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?**

Not applicable.

8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other**

Not applicable.

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

Not applicable.

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

The Deputy Coordinators for International Information Programs.

ADDITIONAL COMMENTS: *(optional)*