United States Department of State

Privacy Impact Assessment

IIP Program Management and Outreach System

(IIP-PMOS – ITAB Number 2600)

Bureau of Administration

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: July 15, 2009

(b) Name of system: International Information Programs Program Management and Outreach System

(c) System acronym: IIP-PMOS

(d) IT Asset Baseline (ITAB) number: 2600

(e) System description (Briefly describe scope, purpose, and major functions):

The **IIP-PMOS** is an umbrella grouping of several systems with varying degrees of privacy information and record subjects. The systems support programs managed by the U.S. Department of State's Bureau of International Information Programs (IIP), in particular, those programs involved with the dissemination of information either internally to the Department or externally to the public. IIP-PMOS includes the following systems:

IIP Results Repository is a website for reporting International Information Programs' accomplishments to IIP senior management for use with other senior Department of State managers and with outside contacts, such as Congress and the White House. Data is captured from Posts and various sections within the Department. The accomplishments are needed to respond to Department or Congressional inquiries or for special reports such as the Office of Management and Budget performance measures. The system is available only on the Department of State's intranet.

The **IIP Tasker** system provides an automated method of tracking and managing IIP taskers (requests for information) generated internally by upper management in the Department's Bureau of International Information Programs and externally by various Department organizations (e.g. Secretariat, Congressional Affairs, Legal). The IIP-PMOS is available only on the Department of State's intranet

Information Resource Center Knowledgebase includes four applications used by Information Resource Centers (IRCs) at Foreign Service posts: a) the IRC Directory describes IRC personnel, collections and services; b) the IRC Annual Plans is a repository of annual plans for IRCs; c) the IRO Consultation Reports is a repository of trip reports produced by regional Information Resource officers during their travel to posts in their region; and d) the Best Practices database.

Information Resource Center Requests captures public diplomacy related reference and research questions posted by the global public and the responses provided by the Department of State's Information Resource Center staff abroad. The global public includes government officials and academia that submit questions via emails or via the system website. The System is used to improve response times to embassies, share

research with other posts and domestic offices and provide a central source for policy related information. It supports the primary purpose of the Information Resource Centers which is to direct timely, authoritative information to targeted foreign audiences in support of U.S. policy goals.

The **Library Professionals** system is a repository of biographical data on speakers who are experts in library science. The system is used as a recruitment tool for posts abroad in that it provides a pool of potential speakers for the U.S. embassies' libraries. The System is available only on the Department of State's intranet.

Reference Requests is used solely as a repository of questions posed by Department of State staff at Posts and answered by staff in the Office of Information Resources. The system is manually updated and not accessible to the public.

Washington File Compiler System (WFCS) is used by IIP editors to assemble compilations of the daily Washington File publications (in regional editions and multiple languages) from individual text items produced or acquired by IIP writers. The application outputs the Washington File in plain text, HTML, and XML versions for distribution over the web, posting on a listserv and replication to overseas Posts.

Distribution Record System and **Tracker** and are both under the IIP Program Management and Outreach System umbrella of systems but outside the scope of this IIP-PMOS Privacy Impact Assessment.

The **Distribution and Record System** is outside the scope of this document as it contains information only on non-U.S citizens. It contains the names, interests and current contact data for all target audience members (those people and organizations believed to have influence on attitudes and actions related to U.S. policy interests).

Tracker is outside the scope as it has its own Privacy Impact Assessment (Speaker and Specialist Program [TRKR – ITAB Number 601]). Tracker supports IIP's Speaker and Specialist Program.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): Not applicable – not a significant modification.

(h) Date of previous PIA (if applicable): June 2008

3. Characterization of the Information

The system:

- ☐ does NOT contain Personally Identifiable Information.
- ☒ does contain Personally Identifiable Information.

a. What elements of Personally Identifiable Information (PII) are collected and maintained by the system? What are the sources of the information?

There are two distinct levels of PII data for systems within IIP-PMOS.

One level involves multiple PII data elements on members of the public. The Library Professionals system falls in this level. It collects and maintains the following elements of PII:

- Academic and Professional Training (Degree, Year, Subject, School)
- Biography / Resume
- Business Address
- Business (Organization) Name
- Business Phone
- Cell (mobile) cell phone
- Email(s)
- Expertise Types and Levels
- Language(s) and Capability (Reading, Speaking, Writing)
- Name (First, Middle, Last, Suffix, Title)
- Organization Affiliations
- Position
- Telephone – Home
- Webpage

The second level of PII data solely includes an individual's contact information. The IIP-PMOS systems that fall within this level and the contact information of which is only official contact information of federal employees are:

- IIP Tasker
- Information Resource Centers Knowledgebase
- IIP Results Repository
- Reference Requests

The system that falls within this level and the contact information is both official contact information of federal employees and general contact information of non-U.S. citizens is:

- Washington File Compiler

And the final system that falls within this level and the contact information is both official contact information of federal employees and general contact information of U.S. citizens is:

- Information Resource Centers Requests

This second level of PII data includes the following elements of PII:

- Address (Business or Home)
- Email

- Name
- Telephone (Business or Home)

b. How is the information collected?

For Library Professionals, data is collected by Department of State Information Resource Officers either directly from subject individuals or indirectly via the Department's Office of the U.S. Speaker and Specialist Program (TRKR). The Officers then manually update the Library Professionals system with the biographic data. Information Resource Officers can add or change the biographical records while users on the Department's intranet can only view the data. Subjects cannot directly update or view their information posted in the system as it is available only on the Department's Intranet (internal network). Subjects can amend their biographic information by contacting IIP directly.

For IRC Requests, non-U.S. citizen contact data is collected directly from the subject when questions are automatically uploaded into the system via incoming email and /or a web interface. The contact data for the IRC staff responding to the Request is entered directly into the system by the responder.

For IIP-PMOS systems covered in this document that collect contact information on the federal workforce, that contact data is either entered into the systems by the subjects themselves or is entered by Department of State staff supporting the respective program and office from the global address list.

c. Why is the information collected and maintained?

For Library Professionals, the information is collected and maintained for overseas Posts in order to have a pool of Speaker candidates at the U.S. embassy libraries.

For other IIP-PMOS systems, the contact information is collected and maintained to provide the user with a means to contact the subject individual or the submitter if needed.

d. How will the information be checked for accuracy?

Information collected directly from the record subject is presumed to be accurate. The contact information about an individual is collected from Department of State records and through interviews with the subject individual.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 5 U.S.C. 301 (Management of the Department of State);
- 22 U.S.C. 1431 et seq. (Smith-Mundt);
- United States Information and Educational Exchange Act of 1948, as amended;
- 22 U.S.C. 2451-58 Fulbright-Hays Mutual Educational and Cultural Exchange Act of 1961, as amended;
- 22 U.S.C. 2651 a (Organization of the Department of State); and
- 22 U.S.C. 3921 (Management of the Foreign Service).

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Information collected and maintained by Library Professionals is the minimum amount of information necessary to identify potential Speakers for future consultations at U.S. embassy libraries.

Information collected in other IIP-PMOS systems is the minimum amount of information necessary to be able to contact the subject individual or submitter if needed.

Because personally identifiable information is collected and maintained by IIP-PMOS, appropriate management, technical and operation security controls are in place to ensure the confidentiality and integrity of the data. Access is available only to authorized Department of State employees performing sanctioned duties. Users must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security. Access to computerized files is password-protected. The computerized files are available only on the Department of State intranet.

4. Uses of the Information

a. Describe all uses of the information.

For Library Professionals, the information is used by posts abroad in order to have a pool of potential candidates for future consultations (speaking engagements) at the U.S. embassies' libraries. From within the system, the individual record of the subject candidate can be retrieved by their name. The system does not collect any social security numbers, passport numbers or visa numbers with which to identify the subject individual.

For other IIP-PMOS systems, the contact information is collected and maintained to provide the user with a means to contact the subject individual or submitter if needed.

There is no placement of Personally Identifiable Information on portable computers. Authorized system users who telecommute can only access the system through the Department of State's secure access using the ONE system with two-factor authentication where one of the factors is provided by a fob with a use-once password.

b. What types of methods are used to analyze the data? What new information may be produced?

The data in IIP-PMOS is not used for analytical purposes. No new information may be produced, except high-level statistics for program reporting purposes sent to the White House and Congress as required.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

IIP-PMOS does not use commercial information, publicly available information, or information from other Federal agency databases.

d. Are contractors involved in the uses of the PII?

Contractors are involved with the operational maintenance of the system. Contractors use the data in IIP-PMOS consistent with the statutory purposes, and do not produce any additional data. Privacy Act contract clauses are inserted in their contracts and other regulatory measures are addressed. Rules of Behavior have been established

and training given regarding the handling of PII information under the Privacy Act of 1974, as amended.

Contractors are employed by the U.S. Department of State within the Bureau of International Information Programs as members of staff to support Bureau programs. All contractors, whether technical or direct program support, must pass a government background check prior to having system access. Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

Data collected and maintained by the IIP-PMOS is only used for purposes related to the IIP Information Resource Centers Program, to creation of the Washington File Compilation System and to IIP internal task assignments. The information is not analyzed or disseminated for any other purpose. IIP-PMOS does not provide flexibility of features that might initiate a functional vulnerability creep or threat.

Authorized employees are assigned level-of-access roles based on their job functions. Roles limit the update and printing capabilities to those deemed necessary for specified job functions.

5. Retention

a. How long is information retained?

These records will be maintained until they become inactive, at which time they will be destroyed or retired in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

A potential risk may occur when a programmed Speaker has out-dated information in the Library Professionals system. This risk is mitigated through the requirement that Information Resource specialists must validate with the Speaker all personal information for correctness and completeness prior to the next speaking engagement of the Speaker.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

Information is shared with U.S. Department of State's overseas posts, embassies and Information Resource Centers that request a library science Speaker in order for them to prepare for the program. Data shared is the individual's name, biography and contact information. No passport, visa or social security numbers are collected or maintained in any IIP-PMOS systems.

Information is also shared with Information Resource Center staff and the Information Resource Office in response to questions on Department policy and guidance. Questions and clarifications come from Department of State staff at embassies and

Posts, from within the Department's International Information Programs Bureau and from the overseas public.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared via phone calls and emails. Information is also shared by authorized U.S. Department of State staff using the same IIP-PMOS systems on the Department's internet.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

When shared within the Department, all information is still used in accordance with IIP-PMOS' stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All IIP-PMOS systems are internal to the Department of State. The public does not have direct access to any of the systems.

All employees of the Department of State have undergone a thorough personnel security background investigation. Access to Department of State facilities is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

Only information in the context of news articles is shared with subscribers (individuals or organizations) abroad via a listerv secured by the Department. The Washington File Compilation System exports a file which is transmitted to the Department's listserv. The listserv has limited access by authorized subscribers in the global public. Voluntarily, subscribers can post their contact information on the public-domain listserv dedicated for the Washington File Compilation System. Otherwise, information is not shared with external organizations.

When members of the public (e.g., journalists, academia) request information on U.S. policy or ask Public Diplomacy related reference and research questions, that information is recorded internally into IIP-PMOS and never transmitted directly out of the system back to the public. That being said, the information is transmitted using the Department of State's email system to the global public who does not have access to the Department's Intranet.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information is shared via phone calls and emails. Except for the Washington File Compilation System, there is no direct sharing of information from IIP-PMOS to outside

the Department. All communication is completed via secure U.S. Department of State communication channels.

The Washington File Compilation System posts news articles written by IIP staff onto dedicated listservs. Communication with the listervs is one-way – it only goes out from the Department onto the listervs from where public subscribers can retrieve information. The listervs hosted by the Department are in a firewall-protected and secured area with limited and defined access by the public. There is no personally identifiable information posted on the listervs.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

Risks to privacy are mitigated by limited access to and release of personal information on a need-to-know basis. IIP-PMOS only transmits information externally via email when responding to reference and research questions from staff at Information Resource Centers and via Washington File Compilation System listervs to the overseas public. In the case of the Washington File Compilation System, the only Personal Identifiable Information available to the public is the writer's name.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

Speaker/Specialist Program Records. STATE-65

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

A Privacy Act Statement is available for those individuals that provide this information by form and notice is also given through System of Record Notice 65.

b. Do individuals have the opportunity and/or right to decline to provide information?

The individual may decline to provide the required information; however, such actions may prevent them from participating in the Library Professionals program.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Conditional consent is not applicable to the official purpose of IIP-PMOS.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notification is provided to the Public via System of Records Notice State-65.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Individuals who wish to gain access to or amend records pertaining to themselves should write to the Director, Office of Information Programs and Services; Department of State; SA-2; 515 22nd Street NW; Washington, DC 20522-6001. The individual must specify that they wish the Cultural Property Advisory Committee Records to be checked. At a minimum, the individual should include: Name; date and place of birth; social security number; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record, and the approximate dates which give the individual cause to believe that the Office of International Information Programs has records pertaining to them.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

Procedures are available for individuals to access or amend records they believe are incorrect. The notice is reasonable and adequate in relationship to the system's purpose and use.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Information Resource Officers determine, on a case by case basis, who in the Information Resource Office and Information Resource Center staff is authorized to access the system and at what level. The level of access and capabilities permitted is restricted by the role assigned to each individual user. Some users are granted read-only access if they have no need to update system records. The separation of roles with different access privileges is in accordance with NIST Special Publication 800-53.

All authorized staff using the system must comply with the Department of State's general "appropriate use policy for information technology". Rules of behavior and consequences, and system use notifications are in accordance with the Privacy Act (subsection e[9]) and OMB Circular A-130, Appendix III.

The security controls in the system are reviewed when significant modifications are made to the system, but at least every three years.

Access to IIP-PMOS is restricted to Department of State personnel that are approved to use the Department's intranet. Only personnel with an approved ID and password can update the Library Professionals system. Only editors and copy desk personnel with an approved ID and password can submit articles and update data for the Washington File Compilation System which outputs data to a listserv and for upload to the America.gov public website.

Department of State system users must pass a government background check prior to having system access. At a minimum, they must possess a security clearance level of confidential, with secret preferred. Annual, recurring security training is practiced and conducted through Diplomatic Security.

Authorized user login identifiers are appended to any system records created or updated, along with the date and time of the record creation or change. This allows administrators to identify the source of any incorrect of incomplete data as recorded in the system.

Contractors authorized to access the system are governed by contracts identifying rules of behavior for Department of State systems and security. Contracts are reviewed upon renewal by management and contract personnel expert in such matters.

b. What privacy orientation or training for the system is provided authorized users?

Annual, recurring security training is practiced and conducted through the Bureau of Diplomatic Security.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform--on an information system.)

The certification and accreditation process independently verifies and validates the application system security controls. Administrative procedures, including independent security investigations of Department applicants and assignment of unique system access rights to individuals, limit access to the system.

There is little residual risk related to access, in particular because the system is available only on a Department of State intranet and there is minimal and controlled direct electronic transfer of data between IIP-PMOS and hosts accessible to external organizations or individuals.

11. Technologies

a. What technologies are used in the system that involve privacy risk?

All hardware, software, middleware and firmware are vulnerable to risk. There are numerous management, operational and technical controls in place to mitigate these risks. Applying security patches and hot-fixes, continuous monitoring, checking the national vulnerability database, following and implementing sound federal, state, local, department and agency policies and procedures are only a few of safeguards implemented to mitigate the risks to any information technology.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Information is transmitted via email quite frequently. A potential risk includes an email containing personally identifiable information inadvertently sent to an unauthorized recipient.

To mitigate this risk, Department of State staff receives training and notifications warning of phishing scams to obtain personal data.

12. Security

What is the security certification and accreditation (C&A) status of the system?

As a component system to the International Information Programs, Program Management and Outreach System, IIP-PMOS was granted Full Accreditation at the Sensitive-But-Unclassified (SBU) level in May 2007. The authorization is valid for up to 36 months. This Accreditation expires on May 31, 2010, or upon significant change to the system, application, or environment.