1. Contact Information

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

2. System Information

(a) Date PIA was completed: July 7, 2009

(b) Name of system: Speaker's Program Database TRACKER

(c) System acronym: TRKR

(d) IT Asset Baseline (ITAB) number: 601

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

Major Functions: The TRACKER system is a central data repository for the Department of State's U.S. Speaker and Specialist Program managed by the Bureau of International Information Programs (IIP). Each year IIP's Worldwide Speaker Program organizes around 1,300 speakers, digital video conferences, webchats and interactive outreach programs to facilitate communication for posts worldwide. All U.S. Speaker and Specialist Grantees must be U.S. citizens. Major components of this program include: Travel Speakers, Strategic Speaker Initiative, Digital Video Conferences and Interactive Electronic Speaker Programs.

- Traveling Speakers — Having an expert from the United States speak to foreign audiences is a compelling way for posts to deliver messages about U.S. policy, society, or culture. IIP Programs hundreds of speakers each year to posts around the world.
- Strategic Speaker Initiative — A centerpiece of Traveling Speakers, this is initiative focus on global policy priorities provides flexibility to IIP and posts in meeting critical speaker needs and encourages regional cooperation among posts in planning and implementing programs.
- Digital Video Conferences — IIP can help posts to reach out to audiences with live interactive video conferences with key experts. In some cases, telepress conferences are just as effective — especially for radio journalists — and matched to the host country's technological base.
- Interactive Electronic Speaker Programs — Webchats, blogs, and podcasts are some of the ways IIP's Speaker Program is expanding our dialog with foreign opinion leaders, both geographically and over time.

The Tracker System stores bios and curricula vitae on participating and potential speaker and specialists. It tracks the funding, authorization, significant communications and evaluations for: traveling speakers, digital video conferences, electronic telepress conferences and webchats. The System is also used to initiate and produce individual grants, to provide a business workflow for Speaker projects and to monitor expenditures for U.S. Speaker and Specialist Program Office (R/IIP/S) services requested by DoS field posts throughout the world. Tracker is a closed accounting system, with manual re-entries into the U.S. Department of State's General Financial Management System.

(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):

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

3. Characterization of the Information

The system:

□ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The following are elements of PII collected and maintained in TRACKER on individuals who are participating as speakers or presenters in the International Information Programs (IIP) Speaker and Specialist Program:

- Name of Speaker/Specialist;
- Date and place of birth;
- Gender;
- Address;
- Telephone, cell, fax numbers;
- Social Security, passport, visa numbers;
- Education; and
- Financial transactions

  Tracker maintains the individual's social security number and payment amount and includes them on the generated Public Voucher for Purchases and Services Other than Personal (Standard Form 1034A). The form is used internally to authorize and verify payment to the speaker.

  Outside the system, the Automated Clearing House (ACH) Vendor/Misc Payment Enrollment Form (Form SF-3881) is completed with the speaker's contact information and social security number, as well as the their bank routing number, account number, contact information.

b. How is the information collected?

Data is collected directly from the record subjects. Additional data may be collected from publicly available information on the internet and through media reports. The U.S. Speaker and Specialist Program staff use the internet to obtain bios, read papers, interviews, and articles written by potential speakers, and to look at lectures on YouTube.

ACH information is obtained over the phone by the U.S. Speaker and Specialist Program staff, or the grantee faxes/emails the completed form back to the program officer.

All collected data is manually entered by the International Information Programs staff.

c. Why is the information collected and maintained?

The information is collected and maintained to recruit speakers, process individual grants, schedule travel and engagements, manage financial accounting, make payments to speakers as compensation for their time, and summarize results for government reporting requirements.

d. How will the information be checked for accuracy?

Information collected directly from the record subject is presumed to be accurate. The information about an individual is collected from Department of State records and interviews with the subject individual. If the subject's social security number and banking information do not match, payment cannot be made to the 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 TRKR is the minimum amount of information necessary to fulfill IIP's statutorily mandated Speakers and Specialist Program. The information is required to award individual grants, make payments to individuals, draft itineraries, plan and program Speaker activities, manage financial accounts, and obtain required visas.

Social security information and other sensitive elements of PII are collected in order to fulfill payment and coordinate with the record subjects' financial institution of choice, and obtain any necessary visas or travel documents. Data is checked for accuracy as submitted by the record subject and is verified against Department Records where appropriate.

Since sensitive PII is collected and maintained by TRKR, 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 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.

The information is required to award individual grants, make payments to individuals, draft itineraries, plan and program Speaker activities, manage financial accounts, and obtain required visas.

Within the system, the individual record of the Speaker can be retrieved by their name in actual practice. There is no retrieval of records by the Speaker's social security number, passport number or visa number.

There is no placement of personally identifiable information (PII) 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-one password.

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

The data in TRKR 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.

The system uses information from the U.S. Department of State Visa and Passport Offices for visa requirements. The U.S. Office of Personnel Management provides per diem and travel rates.

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 TRKR 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 regarding the handling of PII information under the Privacy Act of 1974, as amended.

Contractors are also employed by the U.S. Department of State within the Bureau of International Information Programs as members of staff to support Bureau programs, including the IIP Speaker and Specialist Program.

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 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 Speaker and Specialist Program (TRKR) is only used for purposes related to the IIP Speaker and Specialist Program. The information is not analyzed or disseminated for any other purpose. TRKR 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. When the records become inactive, they will be destroyed or retired in accordance with the Department's published records disposition schedules, as approved by the National Archives and Records Administration (NARA).

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 Tracker System. This risk is mitigated through the requirement that program officers must validate with the Speaker all personal information for correctness and completeness prior to their next speaking engagement.

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 posts abroad that requested the Speaker Program in order for them to prepare for the program. Data shared is the individual's name, biography, travel itinerary and e-mail address. No passport, visa or social security numbers are shared.

If a Country Clearance is requested, it comes from the Speaker and Specialist Program staff in Washington, DC to the post to ensure that the Speaker has permission to enter the country under embassy auspices. This communication is outside and separate from the Tracker System. The Speaker staff enters the request in eCountry Clearance, a separate system on the Department of State's intranet.

The U.S. Speaker and Specialist Program staff completes the Automated Clearing House Vendor/Miscellaneous Payment Enrollment Form with the speaker's contact and banking information and fax the form to the U.S. Financial Payment Center in Charleston, SC facility. The original form is kept by Speaker Program staff for 3 years and then shredded on-site.

This form is not generated from Tracker. The Charleston Center processes the form and initiates payment to the speaker's account by entering the required information into the Department's General Financial Management System.

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

The information shared with the Financial Payment Center is faxed from Department equipment and phone lines. After staff receives the returned form with verification of payment, the form is shredded.

Other information is transmitted using the Department of State's e-mail system.

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 Tracker's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. Faxed documents are destroyed upon receipt once payment verification is received.

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?

Information is shared with Atlas Visa Service, Inc. to process visas required by Speakers for their travel abroad. Data shared is the individual's name, place and date of birth, address, passport number and date of issuance, and travel itinerary. The individual's social security number is not shared.

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

Information is shared with Atlas Visa, Inc. via phone calls, emails and faxes. All communication is completed via secure Department communication channels.

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 to Atlas Visa, Inc. As a vendor of the U.S. Government, Atlas

Visa, Inc. and employees maintain a government security clearance. Information is only released on a “need-to-know” basis to Atlas Visa, Inc. under a statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose.

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 IIP Speaker and Specialist 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 TRKR.

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.

Notice is provided to individuals as part of the Grant Award Letter, and a Privacy Act Statement is available on all forms. Furthermore; 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?

The Tracker Functional Administrators determine, on a case by case basis, the employee on the Speaker and Specialist Program staff who is authorized to access the system. The level of access and capabilities permitted within the system 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. Others are restricted from updating financial data. 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.

E-authentication is used to identify the Tracker user as authorized for access and as having a restricted set up responsibilities and capabilities with in the system. When the user initiates the system, their secure network login credentials are passed to the system via Active Directory. By having a Department of State email account, their network login credentials are checked against authorized system user role membership and access privileges are restricted accordingly.

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 contacts 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 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 no direct electronic transfer of data between Tracker and 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, Speaker and Specialist Program 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, Tracker 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.