PRIVACY IMPACT ASSESSMENT

Bureau of Educational and Cultural Affairs Speaker Program Resource Center Privacy Impact Assessment

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: 12/2022
(b) Name of system: Speaker Program Application Resource Center
(c) System acronym: SPARC
(d) Bureau: Educational and Cultural Affairs
(e) iMatrix Asset ID Number: 327950
(f) Child systems (if applicable) and iMatrix Asset ID Number: Non-applicable
(g) Reason for performing PIA:

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

(h) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?
☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(c) Describe the purpose of the system:

The SPARC system stores contact information and biographical data/curricula vitae on participating and potential U.S. Speakers. This information is shared via email only with the cooperative agency that is responsible for logistical aspects of program administration (including travel bookings and ticketing, funding disbursement and passport/visa arrangements). SPARC is also a repository for program requests, significant

communications with speakers and field posts, and evaluations for all travelling and virtual U.S. Speaker programs and participants. The system captures program details, calculates and summarizes costs, provides a business workflow for speaker projects, and monitors allocations and expenditures on a field post, regional and global basis. The system produces critical statistical reports on programs and budget. SPARC is a closed accounting system, with manual re-entries into the U.S. Department of State's Global Management System (GFMS). Access to SPARC is limited to Department of State direct hires, cleared contractors, and speakers recruited for travelling and virtual programs. There are two types of speakers in SPARC:

(1) Traveling Speakers (U.S. government employees and/or non-U.S. government employees) - Bringing an expert from the United States to speak to foreign audiences is a compelling way for field posts to support U.S. foreign policy, and to communicate with foreign audiences about American society, institutions, and culture.

(2) Virtual Speaker Programs – (U.S. government employees and/or non-U.S. government employees) ECA engages key foreign audiences through live interactive program platforms, including video, web chats and social media.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

PII is collected by SPARC for a business purpose. The following list itemizes the PII collected from speakers that are U.S. government employees and speakers that are non-U.S. government employees.

1. PII about speakers that are U.S. Citizens (U.S. government employees): Name (Last, First, Middle Names; Suffix), date of birth, passport number, photograph, employment information, work email, work title, work phone number, work address and educational information.

2. PII about speakers that are U.S. Citizens (non-U.S. government employees): Name (Last, First, Middle Names; Suffix), date of birth, passport number, photograph, employment information, personal phone number, personal email address, personal home address, and educational information.

For both government and non-government speakers, there is a section in SPARC that requests emergency contact information. This individual designated by the speaker is either a family member or friend and the information requested of them could include the following: Name (Last, First, Middle Names; Suffix), personal/work home phone number, personal/work cellphone number, and/or personal/work email address.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 5 U.S.C. 301 (Management of the Department of State)

- 22 U.S.C. 1431 et seq. (United States Information and Educational Exchange Act of 1948, as amended; Smith-Mundt Act)
- 22 U.S.C. 2451-58 (Mutual Educational and Cultural Exchange Act of 1961, as amended; Fulbright-Hays Act)
- 22 U.S.C. 2651a (Organization of the Department of State)
- 44 U.S.C. Chapter 35 (Paperwork Reduction Act)
- 22 U.S.C. 3921 (Management of the Foreign Service)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number, etc.)?

☒Yes, provide:

- SORN Name and Number:
  Speaker/Specialist Program Records, State-65

- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):
  December 10, 2009

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Office at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No
(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

If yes provide (Consolidate as much as possible):

- Schedule number (e.g., (XX-587-XX-XXX)):
  A-37-010-02

- Disposition Authority Number:
  N1-059-09-11

- Length of time the information is retained in the system:
  Temporary: Cutoff at end of fiscal year. Destroy 50 years after cutoff.

- Type of information retained in the system:
  Speaker/Specialist Program Records:

  Data on U.S. Speakers and U.S. Speaker programs data.

Records could contain biographic information about the speaker/specialist including names, social security, passport numbers, contact information, education and professional experience, financial information, correspondence between the subject, the Department and overseas posts regarding the subjects participation in the program; travel itineraries and visa documentation; grant authorization numbers and types; copies of the grant documents; cost and fiscal data; payment vouchers; country clearance telegrams; and, when available, program evaluations and speaker reports.

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☒ Other
☐ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☐No ☒N/A

- If yes, under what authorization?

(d) How is the PII collected?

Speakers will have access to the application where they can directly enter their own information; if unable to enter their information for some reason, they will provide the information on the U.S. Speaker Information Form (via email attachment) to the U.S. Speakers Office Program Officer to manually enter the information into the SPARC system for them.

(e) Where is the information housed?

☐ Department-owned equipment
☒ FEDRAMP-certified cloud
☐ Other Federal agency equipment or cloud
☐ Other

- If you did not select "Department-owned equipment," please specify.

Although the information system is not housed on the Department owned equipment, it is Government-Owned, Government-Operated (GOGO). SPARC will be housed within SE-AWS GovCloud's heavily access-restricted datacenter cages within each facility in geographically diverse locations within the USA. Multiple layers of physical access control, authentication, and authorization are required before personnel or information system components are permitted access. Further, SE-AWS GovCloud has dedicated multi-tenant security appliances and network area storage units to segregate Federal Agency data from other AWS GovCloud customers.

(f) What process is used to determine if the PII is accurate?

The information is provided directly by the record subject and is presumed to be accurate. It is the record subject's responsibility to provide accurate information. U.S. Speakers Office Program Officer review the information provided by the record subject and verify with the record subject if any clarification is needed.

If record subjects are unable to input their information into the system themselves, then they fill out the U.S. Speaker Information Form and provide it, via email, to the U.S. Speakers Office Program Officer. The U.S. Speakers Office Program Officer then manually inputs the speaker's information as provided in the form directly into the SPARC system. The U.S. Speakers Office Program Officer will follow-up with the record subject as needed to clarify any of the form information.

(g) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

The PII is verified by the relevant Program Officer. Individuals to whom the PII applies are responsible for ensuring the accuracy of their data and have access to their own information to make corrections or updates as needed. All information collected is current as of the collection date and no additional steps are taken to ensure it remains current.

(h) Does the system use information from commercial sources? Is the information publicly available?

No, the system does not use information from commercial sources and the information is not publicly available.

(i) How was the minimization of PII in the system considered?

A potential privacy risk involves unauthorized access to a speaker's name, address, date of birth and biographical information. Information collected and maintained is the minimum amount of information necessary to fulfill ECA's statutorily mandated U.S. Speaker Program. The ECA Executive Office conducted a bureau-wide review in spring 2021 to minimize the collection of PII and safeguard the data in compliance with Department guidelines that required sign off by each Deputy Assistant Secretary.

5. Use of information

(a) What is/are the intended use(s) for the PII?

The information described in 3(d) is required to draft itineraries, plan and program speaker activities, and manage financial accounts.

(b) Is the use of the PII relevant to the purpose for which the system was designed or for which it is being designed?

Yes, the information collected in 3(d) for the system entirely supports the U.S. Speaker Program. The program staff rely entirely on the SPARC system to manage speaking programs.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?

(2) Does the analysis result in new information?

(3) Will the new information be placed in the individual's record? ☐Yes ☐No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐Yes ☐No

(d) If the system will use test data, will it include real PII?

☐Yes ☐No ☒N/A

If yes, please provide additional details.

6. Sharing of PII

(a) With whom will the PII be shared internally and/or externally? Please identify the recipients of the information.

Internal:

The information mentioned in section 3(d) is shared with the U.S. Department of State's overseas Post(s) and the Bureau of the Comptroller and Global Financial Services, Global Financial Services Center (CGFS/GFSC) for programs budgets.

External:

Information mentioned in section 3(d) pertaining to non-USG and USG speakers that belong to Legislative and Judicial branch, will be shared with World Learning and Seven Corners Inc. as they handle all travel arrangements.

(b) What information will be shared?

Internal:
The following PII mentioned in 3(d) for non-government and government U.S. citizens will be shared with the U.S. Department of State's Overseas Post(s) that request the program, and the Bureau of the Comptroller and Global Financial Services, Global Financial Services Center (CGFS/GFSC) for programs budgets: Name (Last, First, Middle Names; Suffix), date of birth, passport number, photograph, work email, work title, work phone number, work address, and educational information.

External:
World Learning (PII on both non-government and government U.S. citizens): Speaker's name, date of birth, address, work email address, passport number, photograph, work title, work address, educational information, and phone number.

Seven Corners Inc. (PII on both non-government and government U.S. citizens): speaker's name, address, phone number, email address and proposed travel itinerary for ECA's Accident and Sickness Program for Exchanges (ASPE).

(c) What is the purpose for sharing the information?

Internal:
The information in section 3(d) is shared with the U.S. Department of State overseas Post(s) that requested the program for management and logistical purposes.

The information in section 3(d) is also shared with Bureau of the Comptroller and Global Financial Services, Global Financial Services Center (CGFS/GFSC), for program budgets.

External:
Information is shared with World Learning for coordination of the speaker's travel itinerary. World Learning facilitates all travel arrangements (itinerary coordination) for judicial branch speakers, legislative branch speakers, and private sector speakers.

Seven Corners Inc. is the contractor/provider that handles the health insurance for ECA's Accident and Sickness Program for Exchanges (ASPE); they issue insurance cards and handle all the claims. ASPE provides health coverage for Speakers during traveling programs.

(d) The information to be shared is transmitted or disclosed by what methods?

Internal:
The information is shared via email with U.S. Department of State's Overseas Post(s) that request the program and Bureau of the Comptroller and Global Financial Services, Global Financial Services Center (CGFS/GFSC) for programs budget. All information is shared via email through a secured transmission methods permitted under the Department

of State policy for handling and transmission of sensitive but unclassified (SBU) information.

External:
Information for World Learning and Seven Corners is shared via encrypted email on a case-by-case basis to those with a need to know. This process is deemed as a secured transmission method permitted under the Department of State policy for handling and transmission of sensitive but unclassified (SBU) information.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal:
All internal communications between Overseas Post(s) and CGFS/GFSC are encrypted. Also, need-to-know basis of least privileges is applied ensuring that only individuals with need to know are e-mailed the PII.

External:
All external communications between World Learning and Seven Corners are encrypted. Periodically, security and privacy training inform authorized users of proper handling procedures.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

Pursuant to the Privacy Act, a Privacy Act statement is included on the U.S. Speaker Information Form which is completed by U.S. government employees and non-U.S. government employees, who are U.S. citizens, and serves as a notice.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☒Yes ☐No

If yes, how do record subjects grant consent?

Notice is given via the Privacy Act statement in the application. The individual may decline to provide the required information; however, such actions may prevent individuals from participating in the U.S. Speaker Program.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

Individuals may contact their respective Program Officer or the Bureau of Educational and Cultural Affairs to ask what is recorded about them. The Department's Privacy Act

practices also allow individuals to gain access to their information by contacting the Department's Freedom of Information Act (FOIA) office for copies of the records retained. Details on this process can be found in the covering SORN, State-65.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

Individuals may contact their respective Program Officer or the Bureau of Educational and Cultural Affairs to ask what is recorded about them and request that information be amended if they believe it to be incorrect. In addition, the procedures for requesting correction of information are set forth in SORN, STATE-65.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

During program engagement, Speaker Program staff inform the speaker of procedures to correct their information both orally and via email. The speaker is informed from the beginning of communications that the collected information provided about and by the speaker is maintained in SPARC. The US Speaker Program Officers and Coordinators also remind the speaker to notify the respective Program staff of any changes to that information during the engagement. Notice is also provided to individuals as part of the Grant Award Letter. Finally, notification of procedures to correct information is also provided via System of Records Notices, STATE-65.

8. Security Controls

(a) How is all of the information in the system secured?

The information in the system is encrypted while in transit and at rest. Internal access is limited to only authorized Department of State users, including cleared contractors who have justified need for the information to perform official duties.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

System Functional Administrators – determine on a case-by-case basis, who in the respective office staff is authorized to access the system and at need-to-know basis. System Functional Administrators can create, view, update, and delete all PII mentioned in section 3(d).

Division Chief, Resource Manager, Program Officer, and Producer – can delete, create, view, and update all PII mentioned in section 3(d).

Program Coordinator - can create, view, and update all PII mentioned in section 3(d), but cannot delete any PII.

Read-Only- Users – these can only view all PII mentioned in section 3(d). This role cannot delete PII.

Speakers – can only view their own PII mentioned in section(d). This role cannot delete PII.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Access to data in SPARC is determined and approved by system functional administrators on a case-by-case basis in consultation with the Director and/or Deputy Director of the U.S. Speaker Program. Account request procedures are in place to determine what access users need in order to perform official duties. Also, all authorized staff must comply with the Department of State's general access user policy for information technology.

(d) How is access to data in the system determined for each role identified above?

System Functional Administrators – access is determined and approved by the ECA/EX/IT Director. This is the level of access needed to grant access to other users via roles.

Division Chief, Resource Manager, Program Officer, Program Coordinator, Producers, Speakers, and Read-Only-Users – access is determined and approved by the System Functional Administrators Users must complete a system request form and submit to the Customer Support Help Desk with cc; to the application/system owner. The application/system owner must approve the request and specify what role the new user should have. The level of access and capabilities permitted is restricted by the role assigned to each individual user.

(e) What monitoring, recording, auditing safeguards, and other controls are in place to prevent the misuse of the information?

All PII is encrypted. To prevent misuse of information, role-based access is used to ensure that the levels of access are restricted to specific job functions. Privileges are assigned on a need-to-know basis and follow the principles of least privilege. Splunk monitoring tool will be installed to capture logs. The audit logs will be reviewed periodically, and inactive accounts will be promptly disabled. The audit trail tracks and monitors usage, access, and provides a record of which functions a user performed or

attempted to perform on the information system. The system also scans and monitors for compliance with the Department and outside regulatory security requirements.

(f) Are procedures, controls, or responsibilities regarding access to data in the system documented?

☒Yes ☐No

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

Users are required to complete Cybersecurity Awareness Training (PS800) each year and privacy training Protecting Personally Identifiable Information (PA318) every two years.