Submit the completed PIA to
Privacy's SharePoint Customer Center

Secretary's Phone Book (SPB)

1. Contact Information

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

2. System Information

(a) Name of system: Secretary's Phone Book

(b) Bureau: S

(c) System acronym: SPB

(d) iMatrix Asset ID Number: 143363

(e) Reason for performing PIA: Click here to enter text.

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

(f) Explanation of modification (if applicable): System upgrade

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
☒Yes
☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
The ATO has expired and a recommendation to grant the ATO is pending completion of the PIA in December 2018.

(c) Describe the purpose of the system:
SPB is a teleconferencing system with a contact database used by S/ES-O, the Operations Center, to maintain contact information for foreign and domestic individuals, as well as some Department employees. The contact database and teleconferencing system are used to facilitate communications for the Secretary and senior Department officials in the course of their duties.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:
Names, job titles, phone numbers (business and personal), emails (business and personal), mailing addresses (business and personal), and notes on the best methods of contact of foreign and domestic interlocutors, as well as some Department employees.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?
22 U.S.C. 2651a and 22 U.S.C. 2656

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?
☒Yes, provide:
- SORN Name and Number: SORN has been drafted and is pending clearance.
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): Click here to enter a date.

☐No, explain how the information is retrieved without a personal identifier.
Click here to enter text.

(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 Division 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:
- Schedule number (e.g., (XX-587-XX-XXX)): A-03-006-10
- Length of time the information is retained in the system: Temporary. Delete when supersedes, obsolete, or when customer requests the agency remove the records.
- Type of information retained in the system:
Name and contact information.

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) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☐Yes ☒No (SSNs are not collected)

- If yes, under what authorization?
N/A

(c) How is the information collected?
Operations Center Officers input contact information for frequent interlocutors. Most contact information is obtained via email directly from the person.

(d) 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.

Click here to enter text.

(e) What process is used to determine if the information is accurate?

Department employee contact information is checked against other sources (eDepartment notices of personnel changes etc.) and Operations Center Officers request contact information via email.

Information for contacts outside the Department is updated/verified with staff of interlocutors when preparing a call, or when the staff provides the Operations Center an update. An email request may also be sent to the contact requesting review and validation of their contact information.

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

Operations Center Officers are responsible for correcting contact numbers. Officers only become aware of updates when the contact provides new information such as when an interlocutor's office requests a call with the Secretary and they provide contact information for the call. This contact information will be compared against existing records and updated as needed. Department staff also often send new contact information to the Operations Center when they change offices or posts.

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

The system does not use information from commercial sources. With certain exceptions (cell phone numbers etc.) most of the business contact information is also publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?

Information is routinely collected by sending the contact a standard email template requesting contact details. The email states that the Operations Center is seeking the information.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?

Individuals can choose whether to provide contact information via phone or email and can select what information they share.

- If no, why are individuals not allowed to provide consent?

Click here to enter text.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

Only information necessary to facilitate efficient telephone connections is collected. This is the minimum amount required for the task at hand.

5. Use of information

(a) What is/are the intended use(s) for the information?
To facilitate communications and teleconferences for the Secretary and senior Department officials. Email and telephone numbers are used to coordinate calls with the Operations Center. Physical mailing addresses are not requested of contacts since electronic or telephonic communication is preferred.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes. The system was designed for this purpose.

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

If yes:

(1) What types of methods are used to analyze the information?
Click here to enter text.

(2) Does the analysis result in new information?
Click here to enter text.

(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

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
S/ES-O only shares information with Department or other USG employees with a need-to-know and, in those cases, only shares information that is publicly available (e.g. work phone numbers and email addresses).

(b) What information will be shared?
S/ES-O only shares publicly available contact information for a specific person when requested by name, such as work phone numbers and email addresses.

(c) What is the purpose for sharing the information?
To facilitate communication between Department offices, and foreign and domestic interlocutors.

(d) The information to be shared is transmitted or disclosed by what methods?
By phone or occasionally by email.

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

S/ES-O has a written policy about what information can be shared and with whom. The blanket guidance is that the Operations Center does not give out any personal phone numbers or email addresses. Ops may provide office phone numbers and email addresses for government employees only to other government employees. Foreign contact information is shared only with senior level Secretariat bureau staff.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Sharing of the personal contact information of senior individuals can be a concern. Therefore, S/ES-O only shares information that is publicly available. In extraordinary circumstances, S/ES-O may share contact information for foreign, non-U.S. citizen interlocutors, with senior Department principals.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The system is not connected to the internet or intranet so there is no practical way for individuals to access their own information. They can call or email S/ES-O in order to update contact information or request other changes.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

S/ES-O regularly sends out requests for updated information. Individuals may also contact the Operations Center with corrections.

If no, explain why not.

Click here to enter text.

(c) By what means are individuals notified of the procedures to correct their information?

Email and phone contact information for the Operations Center is listed on the Department's main intranet page. Individuals may contact the Operations Center to request changes to their contact information.

8. Security Controls

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

The system incorporates all DS-mandated security measures. In addition, it is not connected to the internet or intranet.

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

The system can only be accessed by trained, SCI-cleared Watch Officers from inside a SCIF space with access controlled by a DS guard.

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

All user actions are logged by the system. Logs can be reviewed by the Senior Watch Officer at any time it's necessary to review the actions taken by any Officer.

(d) Explain the privacy training provided to authorized users of the system.

All authorized users sign an agreement attesting they will abide by DOS IT policies, including those involving data privacy. All users are trained on S/ES-O's policies regarding sharing of information during functional training and in-processing. All employees with access to the system are required to take the mandatory FSI course PA459, Protecting Personally Identifiable Information.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users? ☒Yes ☐No

If yes, please explain.

The system servers have standard DOS encryption. In addition, they are not accessible remotely since the system resides on a dedicated network.

(f) How were the security measures above influenced by the type of information collected?

Security measures were developed in accordance with the sensitivity of the information collected regarding high level contacts between foreign interlocutors and the Secretary and senior Department officials.

9. Data Access

(a) Who has access to data in the system?

Only authorized users with SCI-access working inside S/ES-O's facility.

(b) How is access to data in the system determined?

Access is authorized by the system owner (S/ES-O front office) after employees sign an agreement saying they will abide by all DOS IT and data privacy regulations.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

Access is restricted to authorized users who have access to all the data in all the contact records. The system owner and system manager have the ability to run reports not available to ordinary users for system maintenance and accountability purposes.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

All data must be accessible to authorized users as they may be asked to connect a call to virtually anywhere on the planet within minutes. The system is isolated on its own network and accessible only from dedicated computers in the Operations Center. Physical access to the Operations Center is restricted to authorized personnel only and enforced by a security guard at the Operations Center entrance.