PRIVACY IMPACT ASSESMENT

Secretary's Phone Book (SPB) 2.0

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: February 2021
(b) Name of system: Secretary's Phone Book 2.0
(c) System acronym: SPB 2.0
(d) Bureau: S/ES-OPS
(e) iMatrix Asset ID Number: 299655
(f) Child systems (if applicable) iMatrix Asset ID Number: Click here to enter text.
(g) 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

(h) Explanation of modification (if applicable): Click here to enter text.

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:

Secretary's Phone Book 2.0 (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 – Organization of the Department of State
22 U.S.C. 2656 – Management of Foreign Affairs

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

☒Yes, provide:
- SORN Name and Number: Secretariat Contact Records, STATE-84.
- SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN): August 24, 2020

☐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 (Consolidate as much as possible):
- Schedule number (e.g., (XX-587-XX-XXX)): A-03-006-10
- Disposition Authority Number: DAA-GRS-2017-0002-0002
- Length of time the information is retained in the system: Temporary. Delete when superseded, 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) 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?
Click here to enter text.

(d) How is the PII collected?

Operations Center Officers input contact information for frequent interlocutors. Most contact information is obtained via email directly from the record subject.

(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.
Click here to enter text.

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

For Department employees, contact information is checked against other sources (eDepartment notices of personnel changes, etc.). For other interlocutors, the Operations Center Officers request contact information via email directly from individuals or their staff.

Information for contacts outside the Department is updated/verified with the staff of interlocutors when preparing a call, or when the staff provides the Operations Center with

an update. An email request may also be sent to the contact requesting review and validation of their contact information.

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

The information is current. Operations Center Officers are responsible for correcting/updating 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 often send new contact information to the Operations Center when they change offices or posts.

(h) 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.

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

Only the minimum amount of PII necessary to meet operational goals is collected. For instance, during the system development requirements phase, it was determined that SSNs are not needed for operation of the system and so SSNs are not collected.

5. Use of information

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

The intended use of the PII listed in 3d is to maintain an up-to-date directory of business contacts to support the Operations Center (S/ES-OPS) in effectively connecting the appropriate person to the right office and person for call connections.

(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 use of the PII is relevant to the purpose for which the system was designed. The purpose of this system is to connect the Secretary and his/her designated advisors with interlocutors throughout the Department and to outside interlocutors as well to conduct daily business. As such, all of the PII on the system is stored within this system for call processing purposes. The PII collected is necessary and only kept so that the system can perform the functions that it was designed to do. No collateral uses exist for the information collected by the system.

(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?
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

(d) If the system will use test data, will it include real PII? ☐Yes ☐No ☒N/A
If yes, please provide additional details.
Click here to enter text.

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 Operations Center only shares information with other Department 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).
External: The Operations Center only shares information with 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?

Internal: The Operations Center only shares publicly available contact information for a specific person when requested by name, such as work phone numbers and email addresses. Contact information for foreign interlocutors is only shared with senior level Secretariat bureau staff.
External: The Operations Center only shares publicly available contact information for a specific person when requested by name, such as work phone numbers and email addresses. Contact information for foreign interlocutors is not shared externally.

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

Internal: To facilitate communication between Department offices, and foreign and domestic interlocutors.
External: To facilitate communication between Department offices, and foreign and domestic interlocutors.

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

Internal: By phone or occasionally by email.
External: By phone or occasionally by email.

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

Internal: The Operations Center 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. The Operations Center may provide office phone numbers and email addresses for government employees only to other Department employees. Contact information for foreign interlocutors is shared only with senior level Secretariat bureau staff.
External: The Operations Center 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. The Operations Center may provide office phone numbers and email addresses for government employees only to other government employees. Contact information for foreign interlocutors is not shared externally.

7. Redress and Notification

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

No, not formal notice in the form of a Privacy Act Statement. However, for Department employees new to an office whose contact information is needed by the Operations Center, an email is sent to the employee requesting their information and qualifying it's "for OPS only usage."

(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?

The record subject is sent an email stating that their contact information is "for OPS only usage". At this point, the record subject can decline or accept to provide their information.
If no, why are record subjects not allowed to provide consent?
Click here to enter text.

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

None, only Operations Center personnel can see this information.

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

☒Yes ☐No
If yes, explain the procedures.

The Operations Center 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.

(e) By what means are record subjects 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 all of the information in the system secured?
SPB 2.0 relies on the inherent security controls native to the Department's Open Network (OpenNet) in addition to the system level security controls. In lieu of single sign-on, SPB 2.0 requires a username and password which prevents unauthorized users from accessing the data. In addition, SPB 2.0 is not connected to the internet.

(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).
Users – Access to SPB 2.0 is restricted to cleared Department of State (DoS) direct hire and contractor employees. DoS employees and contractors receive their access by requesting access from Operations Center leadership in compliance with internal policies. Once access is obtained, they can view all PII mentioned in 3(d) as needed to connect calls.
System Administrators – System administrators create the accounts that access SPB 2.0 and manage the SPB 2.0 servers. System Administrators are granted access via a ServiceNow account request, submitted by their supervisor, which gives them access to the SPB 2.0 servers. System administrators have logon identifications associated with their name that allows for user auditing. System administrators have no access to PII in SPB 2.0.
Database Administrators – Database administrators (DBAs) are responsible for the daily maintenance, upgrades, patch/hot fix application, backups and configuration of the database. DBAs are granted access via a ServiceNow account request, submitted by the DBA supervisor, which gives DBAs their limited technical access. DBAs have limited backend access and have no access to 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.

The system can only be accessed by trained, SCI-cleared Watch Officers with a need-to-know from inside a SCIF space with access controlled by a Diplomatic Security guard. System access is granted via Operations Center leadership in compliance with internal policies.

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

In general, access is authorized by the Operations Center's leadership after employees sign an agreement saying they will abide by all Department IT and data privacy regulations. Specifically, each role's access to PII is based on the principle of least privilege and the job requirements of that role.

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

The system owner and system manager have the ability to run auditing reports (not available to ordinary users) for system maintenance and accountability purposes.

(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.

All authorized users, system administrators, and DBAs sign an agreement attesting they will abide by Department IT policies, including those involving data privacy. All users are trained on the Operations Center's 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 PA318, Protecting Personally Identifiable Information.