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: 02/07/2009

(b) Name of system: Contact Database

(c) System acronym: Contact

(d) IT Asset Baseline (ITAB) number: 654

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

The application stores personnel information about dignitaries for special events with the President and the Secretary of State. It is used to track invitations and invitees for events hosted by the Secretary of State and President.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security re-certification

(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 source of information is high ranking foreign officials, Diplomatic Corps, government officials, members of Congress, military and members of the private sector. Personally identifiable information that is maintained includes names, address, date of birth, email address, and the number from an official government identification (i.e driver's license, passport, government identification, etc) that will be presented when entering the DOS.

b. How is the information collected?

The responsible bureau compiles the guest list as tasked by the Office of the Secretary or Deputy Secretary. Once approved by S or D, the Protocol Office notifies the invitees by phone of a scheduled event and confirms the invitees RSVP.

c. Why is the information collected and maintained?

The information is collected in order to maintain a list of personnel that are invited and to verify those personnel that attend official state function.

d. How will the information be checked for accuracy?

The individuals or their representative are expected to provide accurate information. The individual or a representative will verify and/or provide the Protocol Office with any updates as required.

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

22 U.S.C. 2621-2625

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

The employees and contractors working for the DOS have undergone a thorough background security investigation. Access to the Department and its annexes is controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals with proper escort. Access to computerized files is under the direct supervision and folders are password protected.

4. Uses of the Information

a. Describe all uses of the information.

The information will be used to record the names of those individuals invited to and attending official state functions. The data will be retrieved by an individual name.

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

No new data or previously unavailable data will be created.

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

Not applicable.

d. Is the system a contractor used and owned system?

This is government owned system but contractors are involved in the design and development of the system. All contractors undergo an annual computer security briefing and Privacy Act briefing. All contracts contain approved Federal Acquisition Regulation Privacy Act clauses.

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.

Users have undergone background checks and received training in handling personally identifiable information. Users receive security awareness training annually. Users are restricted to browsing only data that they are authorized to view for official purpose of their duties only.

5. Retention

a. How long is information retained?

Electronic records can be deleted when file copy is generated or when no longer needed for reference or updating. The official records are retired to the Records Service Center at the end of the Secretary's tenure or sooner if necessary. Transfer to the Washington National Records Center occurs after 5 years. Transfer to the National Archives occurs after 25 years.

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

Regular backups are performed and recovery procedures are in place for electronic records. Access to electronic records is restricted to authorized personnel, is password-protected and under the direct supervision of the system manager. When records have reached their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration.

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?

CONTACTS is restricted to specific Department of State direct-hire and contractor employees that have been granted access to the CONTACTS database in order to perform their official duties.

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

All users must have an OpenNet account. Access is enforced by permissions set with the SQL database. User access is controlled by roles as defined in the CONTACTS system and MS SQL database. The system administrator and ISSO are the only employees with direct access to the database.

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

Risks to privacy are mitigated by granting access only to authorized person and permissions.

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?

The information can be shared with the Executive Office of the President, Congress, media organization, and the general public. The names of those individuals invited to and attending official state function can be shared as a record for historical purpose.

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

No outside organization has direct access to the CONTACT database. The information can be provided upon request and approval by the Office of the Secretary or Deputy Secretary, and must be used in accordance with the authorized purpose.

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 the system and the limited release of personal information.

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):

STATE-33, Protocol Records

☐ does NOT contain information covered by the Privacy Act.

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

Individuals are made aware of the uses of the information at the time of collection. Notice is also published in the system of record State-33, Protocol Records.

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

This information is required for only those individuals who accept the invitation to attend the event. Those that chose not to attend can decline to provide information.

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?

See answer above.

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.

The notice mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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?

Procedures for notification and redress are published in the system of record State-33, Protocol Records.

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

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

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?

Internal access to Contact Database is limited to authorized staff having a need for the system in the performance of their official duties. All users maintain a least a SECRET security clearance level in order to gain access to the Department's unclassified computer network. To access records, the individual must first be an authorized user of the Department's unclassified computer network. Each prospective authorized user must first sign a user access agreement before being given a user account. The individual's supervisor must sign the agreement certifying that access is needed in order for the individual to perform his or her official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer prior to assigning the individual a logon. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged and audited. Access to folders that maintain electronic record must be authorized by supervisor. The supervisor will assign the level of permission for each user and restrict the data that may be seen and the degree to which data may be modified.

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

All users are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training yearly in order to retain access.

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.

There are no expected residual risks.

11. Technologies

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

No technologies commonly considered to elevate privacy risk are employed.

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

Not applicable.

12. Security

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

ATO dated May 2008 and will expire May 31, 2011.