# Privacy Impact Assessment
# State Department Reception Tours (SDRT)
# ITAB Asset Number 953

## 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: April 7, 2009

(b) Name of system: State Department Reception Tours

(c) System acronym: SDRT

(d) IT Asset Baseline (ITAB) number: 953

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

The Reception Tours application is an Internet site allowing members of the general public, especially tourists to the Nation's Capital, and their representatives to request reservations to tour the Diplomatic Reception Rooms at the Department of State.

(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):

Upgrading operating system of application servers.

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

N/A

## 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 data collected complies with Bureau of Diplomatic Security policies [12 FAM 371.5] for identification of individuals seeking access to Department of State facilities.

- First Name
- Middle Name (if any; optional)
- Last Name
- Phone Number
- Email Address
- One of the following four data combinations:
  - Driver's license number and state of issuance
  - Government identification number and agency of issuance
  - Military identification number and branch of issuance
  - Passport number and country of issuance

## b. How is the information collected?

The information is entered voluntarily by, or on behalf of, the individual(s) requesting tour reservations directly into the public-facing online form.

## c. Why is the information collected and maintained?

The information is collected and maintained to make reservations for, and verify the identity of, those requesting tour reservations.

## d. How will the information be checked for accuracy?

No verification is made on the email address beyond using it to contact the individual(s) requesting reservations for Diplomatic Reception Room tours. If the email address is incorrect, the requestor does not receive verification of the tour registration. If the identifying identification with data number and organization of issuance provided when the visitor(s) arrive at the Department is not an exact match to that provided to the Reception Tours application, the visitor(s) will not be permitted to take the tour.

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

Special Services Division in the Office of General Services Management (A/OPR/GSM/SS) is responsible for operation of the tours of the Department's Diplomatic Reception Rooms, and maintains the Reception Tours application (https://ReceptionTours.State.Gov) to facilitate visitors requesting reservations for those tours. The information collected by the application is consistent with Bureau of Diplomatic Security policies for identification of individuals seeking access to Department of State facilities (12 FAM 371.5).

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

Reception Tours collects the minimum amount of personally identifiable information necessary to make reservations for, and verify the identity of, those requesting tour reservations.

Data is maintained in the information technology application, which is configured and maintained in accordance with policies and procedures established by the Office of Information Assurance and the Bureau of Diplomatic Security. Data is accessible only to personnel working for the organization owning the application, and only to individuals provided with access to the application itself. Visitor data is reported on hard-copy paper records to employees of the Bureau of Diplomatic Security 48 and 12 hours prior to a tour. Following the tour, disposal of these records is compliant with the policies and procedures for said disposition contained in 12 FAM 622 and 12 FAM 632.

The data collected complies with Bureau of Diplomatic Security policies [12 FAM 371.5] for identification of individuals seeking access to Department of State facilities. Under those policies, the data is identified as "moderate risk" and is independently verified and validated for protection at that risk level.

Most of the data collected is a matter of public record or would be typically exchanged in the course of normal business activity. No information of a financial nature is collected by this application.

## 4. Uses of the Information

### a. Describe all uses of the information.

The data is accessible only to members of the organization maintaining the application, who provide a list of reservations made and identifying data about the visitors to the Bureau of Diplomatic Security, whose employees validate the data and enable the visitors to enter the Department for the tour. Individuals are aggregated in the reservation list by date and time of the tour, and are not retrieved individually.

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

The data is used as described in paragraph (a) above; no new information is produced.

### 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. Are contractors involved in the uses of the PII?

Users of Reception Tours are made up of FTE and contracting staff. All personnel required to abided to regulatory guidelines and have read and follow the Department of State's Rules of Behavior.

### 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.

Reception Tours does not create new information about the record subject. Thus, there are adequate safeguards in place to preserve data accuracy or integrity and avoid faulty determinations or false inferences about the record subject, thereby mitigating privacy risk. There is also no risk of "function creep," wherein with the

passage of time PII is used for purposes for which the public was not given notice. Based on these specific uses that do not create additional information about the record subject, there is minimal privacy risk.

The security controls in place are consistent with federal regulations and guidelines including the Federal Information Security Management Act. The security controls are subjected to independent verification and validation prior to the Chief Information Officer of the Department granting the application with authorization to operate, are reviewed annually and subject to re-authorization every three years.

## 5. Retention

### a. How long is information retained?

The Office of Information Programs and Services (A/ISS/IPS) confirms that Records Disposition Schedule A-11-009-13, "Visitor Control Files," applies and that disposition occurs either two years after the final entry, or two years after the date of the creation of the document.

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

The data retention schedule is compliant with Department policy and adds no significant risk of inadvertent disclosure.

## 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?

No such sharing occurs.

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

Not applicable.

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

Not applicable.

## 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?

No such sharing occurs.

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

Not applicable.

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

Not applicable.

## 8. Notice

The system:

☐ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

☒ does NOT contain information covered by the Privacy Act.

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

Data is provided voluntarily by the individuals.

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

Failure to provide information will result in the individual not being permitted to tour the Diplomatic Reception Rooms.

**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?**

Failure to provide information will result in the individual not being permitted to tour the Diplomatic Reception Rooms.

**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.**

Data is provided voluntarily by the individuals.

## 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?**

Not applicable.

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

No such process exists; no further risks result.

## 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?**

All users accessing the system are employees of the Department of State with current security clearances. Access to the database is tracked in system logs.

**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 accessing 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.**

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.)

Reception Tours is a government owned system supported by contract employees, who support U.S. Government employees in their maintenance of the system.

Contractors who support Reception Tours are subjected to a background investigation by the contract employer equivalent to a "National Agency Check" of the files of certain U.S. Government agencies (e.g., criminal law enforcement and homeland security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

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.

## 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 (NVD), 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.

Reception Tours does not employ technologies that raise the level of privacy risk to the data.

## 12. Security

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

Certification and accreditation of this "moderate risk" data system is pending and should be completed in May, 2009.

## 13. Certifying Officials' Signatures

_____

**System Owner**

_____

**Program Manager**

_____

**Information Security Manager**

***Email the completed PIA in MSWord format to "PIA Team". Upon signing, please send this signature page to the same group email box in the form of a scanned PDF, or send as paper via interoffice mail to the Privacy Office "A/ISS/IPS/PRV".***

_____

## TO BE COMPLETED BY THE PRIVACY OFFICE

**Reviewer:** _____ **Approver:** _____