__Visa Request (VR)__

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 20, 2009

(b) Name of system: Visa Request

(c) System acronym: VR

(d) IT Asset Baseline (ITAB) number: 4391

(e) System description:

CA/PPT's Special Issuance Agency (SIA) is responsible for producing diplomatic, official and no-fee passports for all governmental agencies, including the White House and Congress. They produce tourist passports for these clients as well, and also for constituent referrals from Congress. Part of SIA's mandate is to assist travelers in obtaining visas for official government travel from foreign embassies and/or consulates. In obtaining those visas, the agency tracks and monitors the letters and visa applications sent to and collected from the respective foreign offices. To track those applications, agency staff and couriers use the Visa Request program to produce request letters, track and monitor the status of each request, and schedule deliveries and pickups from the foreign offices.

(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): N/A

(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?

Personally identifiable information that is contained includes: name, date of birth, place of birth, gender, and a passport number.

The source of information for the VR system is U.S. citizens applying for travel documents. Most of the data in VR is taken from a combination of passport info and country specific applications for granting a foreign visa.

b. How is the information collected?

Most of the data in VR is manually entered into the system from a combination of passport information and country specific applications for granting a foreign visa. Each foreign government has its own requirements for visas. The majority of them require the traveler to fill out an application which is unique for that country, some don't require any forms. Some countries require host government approval before they can issue a visa to an official traveler, some don't. All requests require official notification from the State Department that the traveler/employee is going on official travel to represent the U.S. government. A cover letter accompanies the passport, visa form, photos, and any supplemental forms the host country may require. Each country has its own separate form. The majority of the embassies do not contact SIA when a visa is ready. If couriers have delivered a package for processing, they return within the number of days required to process (each one is different) and try to retrieve the passport with the visas. If it is not complete, then VR personnel will reschedule pick up when completed.

c. Why is the information collected and maintained?

The information is collected and maintained to track and monitor the status of visa applications for travelers that travel overseas on official government business.

d. How will the information be checked for accuracy?

The data received from applicants on the application is verified primarily by a review of the applicant’s passport. However, as part of the supporting documentation for assignment travel, applicants may provide copies of travel messages that contain additional PII information such as truncated social security numbers. However, this information is not entered into the VR system and the supporting documentation is only maintained on site for 60 days after issuance of the visa, after which it is destroyed. VR tracks the state of the approved Visa, so no other data is verified.

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

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 8 U.S.C. 1101-1503 (Immigration and Nationality Act of 1952, as amended)
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1185 (Travel Control of Citizens)
- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and assistance to other agencies)

- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries)

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

Given the importance to national security and diplomatic travel, the minimum amount of PII necessary to establish a U.S. Government employee's identity and citizenship status is collected by Visa Request. Visa Request is determined to have a moderate "confidentiality impact level" due to the amount of potential harm that could result to the subject individuals and the organization if the PII in this system were exposed and/or misused. With the collection of passport data, Visa Requests has a high data element sensitivity and high data subject distinguishability. These factors are mitigated through a very specific context of use, in that Visa Requests uses passport information for specific travel arrangements of U.S. Government employees, and through a statutorily mandated obligation to protect confidentiality. Therefore, the confidentiality impact level is moderate.

The collection of passport data is the minimum amount of PII necessary to fulfill the statutory purposes of the system. Any remaining privacy risks inherent in the sources or methods of collection are mitigated by appropriate privacy and security controls detailed throughout this privacy impact assessment.

Specifically, there are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), and audit reports. If these controls are not implemented, non-government employees could engage in criminal activities such as fraud or espionage against the United States Government. Failure to authorize the correct government worker could also endanger all overseas locations with terrorist or criminal activities.

4. Uses of the Information

a. Describe all uses of the information.

The Department of State uses information to request cover letters to foreign embassies, and to track and monitor requests to foreign embassies that are lawfully permitted to issue visas to official representatives traveling on behalf of the U.S. Government. The data collected from the applicant and passport is the minimum amount of PII necessary to produce the required documentation for a foreign embassy or consulate to issue a visa.

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

SIA is the only passport agency with a mandate to provide the Visa approval service, therefore no other agency or entity uses the VR database. The data is not analyzed but checked to make sure requests for visas are for official travel and the application(s) can be routed to the embassies for processing. No new data will be retrieved from the existing passport, nor will any new data be applied to the letters that are provided to obtain the visa. At the final step, the physical passport will return to the applicant, whether an official visa is obtained or not.

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

VR does not use any commercial information, publicly available information, or information from any other Federal agency database.

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

VR is owned by CA/CST/PS, as it's a GOTS product, and has both contractor users as well as government users. The development and maintenance of VR is performed by the Visa Request personnel of Stanley Associates located at:

6363 Walker Lane

Suite 401

Alexandria, VA 22310

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.

Since VR has a very specific use, generating and tracking documents to facilitate U.S. Government employees obtain visas for official travel, the potential privacy risk arising from "function creep" is negligible. Further, since VR does not perform internal analytical functions on the PII, does not create internally new information about the record subject, and does not get data from sources other than the record subject, potential privacy risk is further decreased.

5. Retention

a. How long is information retained?

Per the Department of State's Domestic Records Disposition Schedules, Chapter 13: Passport Records, A-13-002-06 Visa Request System, records within the Visa Request System are used to track and monitor the application process of obtaining visas from foreign embassies and/or consulates for official U.S. government travelers.

Data includes name, date/place of birth, gender, passport number, travel dates, purpose of travel and cities to be visited.

Active records must be destroyed five (5) years after issuance. (DispAuthNo: N1-059-09-25, item 1a.)

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

Visa Request system contains name, date/place of birth, gender, passport number, travel dates, purpose of travel and cities to be visited. The source of information for the VR system is U.S. citizens applying for travel documents. Most of the data in VR is taken from a combination of passport info and country specific applications for granting a foreign visa.

Since Visa Request contains sensitive personally identifiable information, such as passport number combined with data of birth, the data maintained by VR is destroyed after a 5 year period to ensure that the data is not used to unauthorized purposes and reduces the risk of data breach.

Information is shared by secure transmission methods permitted under the Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. VR backup information is protected from unauthorized modification by the physical security and access controls in place at PPT/SIA. VR data is stored on site in a locked server room with cipher lock. Only cleared technical personnel (government and contractors) are allowed to access the server room housing VR servers, and no one is allowed to access the system until the appropriate background screening has been completed.

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 internal organizations share this information.

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

Information is not shared internally.

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

No information is shared internally.

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 external organizations share data with VR.

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

No information is shared outside the Department.

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

No information is shared outside the Department.

Residual risk is accepted through the authorization process.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

□ does not constitute a system of records covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information submitted is described in the System of Records Notices titled STATE-39, Visa Systems.

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

Yes, an individual does have the opportunity or right to decline or provide information. However, if he or she declines, they will not be provided with the consular service they are requesting (i.e. Visa Letter).

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?

The information is used only for the purpose of requesting and tracking the visa. No other uses are provided for VR.

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 data collected is voluntarily given in an effort to complete the Visa Letter, thus, enabling the individual to travel to foreign countries. There are no risks associated with the individual being unaware of the collection, since the applicants are volunteering the information in order to attain the correct travel documentation for official travel abroad.

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?

VR contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records regarding them, how to request access to their records, and how to request an amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of passport records on grounds pertaining to law enforcement in the interest of national defense and foreign policy, if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.32.

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?

Authorized VR users' access is limited to the five user function levels (0-4). These levels allow VR to comply with least privilege and accurately keep track of each user's actions within the VR db server. They also protect the user from having data entered or modified by someone else under the user's identity. Database administrators authenticate to and are authorized by the SQL server application.

The VR system supports six user groups: VR specialists, managers, couriers, office clerks (for express mail), system administrators, and database administrators. The VR admin guide lists the permissions that go with each user level. The user interface and the database both automatically enforce user permissions. Assignment of permissions is done manually by level 3 and 4 users. Level 3 users cannot assign level 4 permissions.

All VR users, including system administrators, receive their access through local access requesting procedures organic to the CA organization and compliant with 12 FAM policies. Each user must submit an account request form indicating the requirement for system administrator privileges. The account request is reviewed by the user's supervisor and must be approved by the VR system manager before the request can be granted.

VR employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals. The auditing reports are generated and reviewed by the database administrator. A subset of audit records, for request history, is available to level 1 users and above via the Trace report, and on the History screen. This allows them to view all events that happened to an individual visa request record.

b. What privacy orientation or training for the system is provided to 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. Upon completion of DS's Security Briefing and CA's in house Security Awareness presentation, attendees are required to sign forms acknowledging that they have read, understand, and agree to abide by the rules of behavior, before obtaining authorized access to the information system and its resident information. Internet based Visa Request users will be required to acknowledge reading and accepting the Rules of Behavior before accessing Visa Request by electronically signing via the Submit button.

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.

Residual risk related to access is the consequence of the inconsistent or overlooked application of the several controls described in this Section. Privacy vulnerabilities are mitigated by effective administrative procedures for access authorization, account housekeeping, and monitoring, recording, and auditing of user activity. VR does not use production PII for any reason other than production purposes, thus de-identifiying or anonymizing the data is not necessary.

VR end-users are required to take DS training for access to OpenNet; media access is also addressed in the Consular Affairs Security Awareness and Training Plan. End users are continuously trained annually with security awareness training to safeguard information system sensitive but unclassified data (SBU) from unauthorized users by storing diskettes, CDs, printouts, etc., in a safe and secure manner. Shredders are provided throughout PPT/SIA for the proper disposal of paper (SBU) medium.

11. Technologies

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

VR is a Government off-the-shelf (GOTS) product and as such meets required security capabilities, design and development processes, required test and evaluation procedures and documentation under the supervision of its Project Manager in accordance to 5 FAH-5 H-110, Developing and Managing Department of State Projects. All CA/CST contracts have input from DS and CA on security matters in accordance to 12 FAM 650, Acquisition Security Requirements for Operating Systems and Subsystem Components.

Since VR resides on the OpenNet, it depends on the IDS that are in place for OpenNet to monitor the inbound and outbound communications for unusual or unauthorized activities or conditions. The operating system for VR is thus configured and maintained according to the State Department's security guidelines and protected by Access Control Lists (ACL).

Additionally, VR uses the following technologies for their database:

SQL Server Logs: archived and moved from the server via Robocopy utility

VR Events table: archived via SQL Server Integration Services (SSIS) package (event records are moved to separate Archive database)

Database SQL access is restricted by the principle of least privilege via database access controls. No user has direct access to the database; the only means is via the application. For the operating system, it's configured and maintained according to State Dept. security guidelines, and all application files and backups are in locations protected by ACLs.

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

Technologies used are inherently unsecured and therefore, a security risk from initial implementation. These technologies, however, are mitigated because they are configured to the correct DS standards and Windows policies created to lock down the system.

12. Security

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

The system was granted Authority to Operate (ATO) 8/31/09 – 8/31/12.