PRIVACY IMPACT ASSESSMENT

Visa Request System

1. Contact Information

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

2. System Information

(a) Name of system: Visa Request System

(b) Bureau: Consular Affairs (CA)

(c) System acronym: VRS

(d) iMatrix Asset ID Number: 4391

(e) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

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 VRS is currently undergoing its Assessment and Authorization (A&A) in order to receive an Authorization to Operate (ATO) status. VRS is expected to receive its ATO by Spring 2021.

(c) Describe the purpose of the system:

The VRS supports the Consular Affairs Passport Services Directorate, Special Issuance Agency (CA/PPT/SIA) in obtaining visas from foreign embassies and/or consulates for official U.S. government travel. The VRS generates formal letters to the foreign embassies or consulates requesting the issuance of a diplomatic or government official visa. The SIA either provides the visa request letters to the employing agency of the person traveling or submits the completed visa application package, including the visa request letter, directly to the foreign embassy/consulate. As part of the process, VRS is also used by SIA to track and monitor the visa request letters and visa applications sent to and collected from the respective foreign

embassies/consulates, as well as to schedule deliveries and pickups from the foreign embassies/consulates.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

VRS contains the following U.S. citizen PII: name, passport information, personal address, birthdate, birthplace, personal and business phone number(s), job title, travel dates, places of travel, and nationality.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 U.S.C. 3927 (Chief of Mission)
- Executive Order 11295, August 5, 1966; (Authority of the Secretary of State in granting and issuing U.S. passports)

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

☒Yes, provide SORN Name and Number:
STATE 26, Passport Records, March 24, 2015

☐No, explain how the information is retrieved without a personal identifier.

(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

A-13-002-06 Visa Request System
Description: The Visa Request System (VR) is a system used to track and monitor the application process of obtaining visas from foreign embassies and/or consulates for official U.S. government travelers.
Disposition: Temporary: Cut off at issuance Destroy five (5) years after cutoff.
DispAuthNo: N1-059-09-25, item 1a

A-13-002-06a Intermediary Records

Description: The Visa Request System (VR) is a tracking system used to track and monitor the application process of obtaining visas from foreign embassies and/or consulates for official U.S. government travelers. Records include: hard copy and electronic input documents or forms designed and used solely to create, update or modify the records in an electronic medium and not required for audit or legal purposes (such as need for signatures) and not previously scheduled for permanent retention in NARA-approved agency records schedule. Also includes adhoc reports output for reference purposes or to meet day-to-day business needs.
Disposition: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.
DispAuthNo, DAA-GRS-2017-0003-0002

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system?

☒ Members of the Public (are US citizens or aliens lawfully admitted for permanent residence)
☒ U.S. Government/Federal employees or Contractor employees
☐ Other (are not U.S. Citizens or aliens lawfully admitted for permanent residence)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☐Yes ☒No

- If yes, under what authorization?

(c) How is the information collected?

The data in VRS is collected in two ways:

1) U.S. government travel orders and/or an official memorandum from the traveler's employing agency, and/or the employee contacts the SIA to provide information necessary to complete the cover letter which will accompany the visa application and the traveler's diplomatic or official passport; and

2) Country-specific visa applications completed by the traveler or the employing agency.

VRS generates cover letters that accompany visa request packages that provide notification from the State Department that the traveler/employee is going on official travel to represent the U.S. government. The letters generated by VRS are considered ancillary in our process, but several foreign countries now consider them to be an essential step in providing visas in U.S. diplomatic and official passports.

(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.

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

The VRS data are verified primarily by a manual review and comparison of the information on:

1) The traveler's diplomatic or official passport;
2) The U.S. government travel orders or an official memorandum from the traveler's employing agency;
3) Country-specific visa applications completed by the traveler or the employing agency; and
4) Previous travel information contained in the Department of State (DoS) Consular Affairs Consular Consolidated Database (CCD) system.

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

The traveler is responsible for ensuring that the information provided is current. VRS staff inputs data into the system provided by the traveler to facilitate the process of receiving a foreign visa.

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

No, VRS does not use information from commercial sources nor is it publicly available.

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

Yes. When a U.S. government employee is preparing to travel and requires a visa, the employee or federal agency contacts the SIA to provide information necessary to complete the cover letter which will accompany the visa application.

The applicant is verbally briefed (phone or in person) on the required notice:

1. The purpose for which the information is required.
2. The possible uses of the information.
3. How the data are protected from unauthorized/ illicit disclosure.
4. The potential consequences if the applicant declines to provide the data (i.e., that his/her visa application may be declined).

(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?

The person who is planning to travel is verbally briefed (by phone or in person) on the required notice which includes the potential consequences if the applicant declines to provide the data (i.e., that his/her visa application may be declined).

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

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

The PII listed in question 3(d) is the minimum necessary to perform the actions required by VRS. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered and addressed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

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

The information in the VRS is used to develop letters for official government travel to foreign embassies/consulates. The VRS tracks and monitors visa requests sent to and collected from respective foreign offices in order to assist U.S. travelers in obtaining visas for official government travel from foreign embassies and/or consulates.

(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 PII is used according to the purpose for which the VRS is designed-- to provide letters for official government travel to foreign embassies/consulates and to track visa statuses.

(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?
(2) Does the analysis result in new information?
☐Yes ☐No
(3) Will the new information be placed in the individual's record?
☐Yes ☐No
(4) With the new information, will the State 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.

Internal Information Sharing:
The term "internal sharing" traditionally refers to the sharing of information within the Department of State (DoS), but external to the owning organization (referred to as a "bureau" at DoS). However, since the various Bureau of Consular Affairs (CA) offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau to protect PII. With that understanding, information in the VRS system will be shared internally with the Consular Consolidated Database (CCD) system.

External Information Sharing:
The VRS does not share information externally.

(b) What information will be shared?

The PII listed in item 3(d) above will be shared.

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

The VRS information is replicated in the CCD system for the current and future use by the Special Issuance Agency (SIA), which validates information and assists in maintaining and verifying information on visa request letters to foreign embassies and/or consulates for official U.S. government travel.

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

Communications between the VRS and the CCD system is database to database and protected using Hypertext Transfer Protocol Secure (HTTPS) with Transport Layer Security (TLS) encryption.

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

Safeguards in place for internal sharing include secure transmission methods permitted by State Department policy for the handling and transmission of sensitive but unclassified (SBU) information. The VRS information transmitted is encrypted as described in paragraph 6(d) above to ensure the security of data transmission.

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

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

Accidental disclosure of information to unauthorized parties. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization, and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

Deliberate disclosure of information to unauthorized parties or theft, regardless of whether the motivation is monetary, personal or other motives.

These risk areas are mitigated using a multi-faceted approach to security:

- Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, sensitive but unclassified, and all higher levels of classification. Users must also sign a user agreement.

- Strict role-based access control based on approved roles and responsibilities, authorization, need-to-know, and clearance level.

- System authorization and accreditation process along with continuous monitoring via the Risk Management Framework. Security controls are implemented for management, operational, technical and privacy functions regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

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

The U.S. government traveler cannot access the VRS system directly. The traveler is verbally briefed (by phone or in person) on how to find out information about themselves and how to

correct it when needed. Applicants can contact the representative who assisted them as well or refer to the following:

- Follow instructions for gaining access as stated in SORN STATE-26.
- Visit the Department of State FOIA website which includes instructions on how to obtain access by contacting the listed offices.

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

☒Yes ☐No

If yes, explain the procedures.

The U.S. government traveler can contact the Department of State representative who assisted them as well as refer to the following:

- Follow instructions for gaining access as stated in SORN State-26
- Visit the Department of State FOIA website which includes instructions on how to obtain access by contacting the listed offices.

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

Individuals are notified of the procedures to correct records in VRS by a variety of methods:

1. During their verbal briefing (by phone or in person); afterwards, individuals may contact the U.S. Department of State representative who briefed them.
2. Published SORN
3. Department of State FOIA website
4. Notifying the Department of State by letter or email that a correction is needed
5. Employing agency internal administrative processes

Each method contains information on how to amend records and contact information.

If no, explain why not.

8. Security Controls

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

The VRS system is secured within the Department of State's internal unclassified network, (OpenNet), where risk factors are mitigated through the use of defense in-depth layers of security including management, operational, technical and privacy security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform their official duties.

Access to VRS is further protected with additional access controls set at the application/database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer (ISSO). The audit vault system is used to monitor all privileged access to the system and violations are reported to senior management daily, if applicable.

The VRS system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institutes of Standards and Technology (NIST) guidance, NIST 800-53, and privacy overlays of management, operational, technical and privacy controls are in place and are tested as part of the continuous monitoring program.

(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.

To access the VRS system, authorized users of the Department of State's unclassified network, OpenNet, require a background investigation and an application approved by the supervisor and the local ISSO. Each authorized user must agree to the user access agreement/rules of behavior before being given a user account. Authorized users are issued a Personal Identity Verification /Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon. Access to the VRS application is controlled via login identifications (IDs) assigned to authenticate users.

Access to the system is role-based, and restricted according to approved job responsibilities and requires managerial concurrence. Local Information System Security officers (ISSOs) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function approved by the supervisor and level of clearance.

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

The CA System Manager and CA ISSO, in conjunction with the CA Security team, periodically scan and monitor the VRS information system for compliance with Department of State Security Configuration Guides and conduct annual control assessments (ACA) to ensure that the system complies with Department of State and federal security policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor VRS for changes or misuse of its information.

In accordance with Department of State Security Configuration Guides, VRS auditing is enabled to track the following events on the host operating systems and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges, and changes in file access restrictions.

The purpose of the audit trail is to document modification of and/or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness Training, which has a privacy component, to access or use systems. Additionally, Department of State personnel are required to take the biennial course PA318, Protecting Personally Identifiable Information. Lastly, the State Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

To combat the misuse of information by personnel, numerous management, operational, technical, security and privacy controls are in place in accordance with applicable National Institute of Standards and Technology guidelines, NIST 800-53, and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit are encrypted, physical and environmental protection is implemented, media handling configuration management is utilized, and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at unauthorized access. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

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

The consequences to organizations or individuals whose PII has been breached or exposed to unauthorized users may include inconvenience, distress, damage to standing or reputation, financial loss to the Department or individuals, harm to Department programs or the public interest, threats to personal safety, and/or civil or criminal violation. The security measures listed above were implemented in accordance with the National Institute of Standards and Technology (NIST) guidelines to secure the data in the system in accordance with federal laws and policies, including Department policies.

9. Data Access

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

VRS Special Issuance Agency staff which consists of 5 different user groups (VRS Administrator, Managers, Visa Lead, Visa level users, and Express Mail user), in addition to the System Administrator and Database Administrator.

VRS SIA Staff: DoS Personnel who manage the information within the system have access to PII data which is role-based.
System Administrator: The System Administrator has access to all data and is responsible for all daily maintenance, establishing personnel access control lists (ACLs), and performing backups.
Database Administrator: The Database Administrator has access to all data and is responsible for the daily maintenance, upgrades; patch/hot fix application, backups and configuration to the database

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

Access is determined based on requests which are approved by the supervisor and the local ISSO. Access is role-based and the user is granted only the role(s) required to perform officially assigned duties.

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

Information is documented in the VRS System Security Plan regarding access to data.

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

Separation of duties and least privilege is employed, and users have access to only the data that the supervisor and the local ISSO approves to perform official duties.

- **VRS SIA Staff Users:**
  - VRS Administrator and Manager – Have access to all information; grants access to the system and can use all features on the administrator screen including visa requests, express mail, access to run all management and express mail reports.
  - Visa Lead and Visa Level user – Have access to all information and can use all features of visa requests, Express Mail, users columns, and can run Express Mail reports.
  - Express Mail user – Have access to traveler address and passport number; visas that are in received, in process, and completed status; dates of travel; and the destination and courier name for visas. This user can view and receive Express Mail screen functions and can run Express Mail reports.

- **The System and Database Adminstrators:** The System and Database Administrators have access to all of the information in the VRS system.

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

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented; access is role-based as required by policy.

- Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- Users are uniquely identified and authenticated before accessing the VRS via dual factor authentication that is required to access and log on to a federal system. VRS activities conducted while logged on can be traced to the person who performed the activity.