Remote Data Entry System (RDS)

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: 10/15/08

(b) Name of system: Remote Data Entry System

(c) System acronym: RDS

(d) IT Asset Baseline (ITAB) number: 87

(e) System description:

The Remote Data Entry System is used at overseas posts of the Department of State (DOS) and authorized remote sites outside of the posts such as travel agencies and banks to support the collection of non-immigrant visa applicant data in a machine-readable form from nonimmigrant visa (NIV) applicants.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

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

☒ PIA Information Review

(g) Explanation of modification (if applicable): Not applicable.

(h) Date of previous PIA (if applicable): 05/25/2007

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?

RDS primarily collects data on foreign nationals as part of the nonimmigrant visa application process. As such, the information provided by the nonimmigrant visa applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

Because NIV applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents) they are not covered by the provisions of the Privacy Act. However, an NIV application may include PII about persons associated with the applicant who are US citizens or legal permanent residents. This PII data may include names of US sponsor/petitioner, US employer, and the names and contact information of US contact person.

b. How is the information collected?

The data is collected on Form DS-156 or DS-160, “Nonimmigrant Visa Application” or Form DS-1648 “A/G/NATO Visa Application.”

After completing the form, the applicant takes the form to an approved office (e.g., travel agency, bank fee collection agents). These off-site offices enter data from the application form using the RDS Client software application and submit the machine-readable data to the post on portable magnetic media, accompanied by the forms and a 1D barcode label. The RDS system also includes the capability to scan a 2D barcode label to automatically populate RDS with NIV application data collected from the EVAF system. The post reviews this data for further processing.

c. Why is the information collected and maintained?

The information is collected to determine the eligibility of foreign nationals who have applied or are applying for a nonimmigrant visa. RDS does not maintain the data once the data is transferred to the post.

d. How will the information be checked for accuracy?

Accuracy of the application data submitted in RDS is the responsibility of the NIV applicant and the RDS Client system user at the off-site location and the visa unit processing the visa.

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

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

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

Due to strict security controls that are required to be in place before operation of the system, no identified privacy risks are associated with this system. RDS collects and maintains only the minimum PII required to perform this determination; therefore, over-collection of PII is not a risk.

4. Uses of the Information

a. Describe all uses of the information.

RDS is a “front end” for the collection of NIV application data overseas. RDS does not maintain application data and PII; rather, the PII and application data is transmitted to the NIV system, usually within a couple of days of the data being received at post. Records are retrieved from RDS by the barcode affixed to the NIV application. Consular officers use the information to make a determination whether to grant a nonimmigrant visa.

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

RDS performs no internal analyses of NIV applications other than error checking to ensure that all required fields are completed and is suitable for transmission to the NIV system.

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

Visa applicant data provided by visa applicants and/or foreign authorities is used to effectively identify the visa applicant.

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

RDS is a government used and owned system. It is supported by Department contract employees, some of whom are located at contractor-owned facilities. All employees and contractors must pass an annual computer security briefing and Privacy Act briefings from DoS and/or the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) 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.

RDS receives all PII directly from the NIV applicant. User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted.

5. Retention

a. How long is information retained?

The PII collected in RDS is not retained beyond the time required to perform error/completeness checks, then it is transmitted to the NIV database, usually within a couple of days of being received at post. PII retention in the NIV database is governed by a separate records retention schedule.

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

Because RDS does not maintain NIV application data beyond the time required to error check the data and transmit it to the NIV database, no privacy risk from a lengthy retention exists.

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?

RDS data is shared with other visa-related information systems operated by the Bureau of Consular Affairs.

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

The PII collected in RDS is transmitted to other visa-related information systems by secure transmission methods permitted under DoS policy for handling and transmitting sensitive but unclassified (SBU) information.

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

Privacy risk from internal sharing is negligible because PII is transmitted to other visa-related information systems by secure transmission methods permitted under DoS policy for handling and transmitting sensitive but unclassified (SBU) information.

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?

As described above, the PII and application data collected by RDS is regularly transmitted to other internal visa-related information systems.

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

The Department does not use RDS to share information outside of the Bureau of Consular Affairs Visa processing environment.

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

Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

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):

- Visa Records. STATE-39

□ Does NOT contain information covered by the Privacy Act.

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

The application forms explain the reason for the information collection, how the information will be used, and potential outcome of not providing information.

The application form provides a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

Also, notice is provided in the System of Records Notice Visa Records, STATE-39.

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

Information is given voluntarily by the applicants and with their consent, by family members and other designated agents.

Individuals who voluntarily apply for a U.S. visa must supply all the requested information, and may not decline to provide part or all the information required, if they wish visa services.

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?

Applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

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 information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The information provided on the nonimmigrant visa application form and in the SORN regarding visa records fully explain how the information may be used by the Department and how it is protected.

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?

The information in RDS is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa applicants may change their information at any time prior to submission of the application to the Consulate or Embassy. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. The Department will release the following information to a visa applicant upon request and this guidance is available to the public in 9 FAM 40.4:

(1) Correspondence previously sent to or given to the applicant by the post;

(2) Civil documents presented by the applicant and

(3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted, i.e., with any remarks or notations by U.S. Government employees deleted.

RDS information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a), and individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN cited in this PIA, and in rules published at 22 CFR 171.31. The procedures inform how individuals may inquire about the existence of records about them, how to request access to records, and how to request an amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for 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.

To the extent information in RDS is Privacy Act covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purposes and uses and its applicable legal requirements. Therefore this category of privacy risk is appropriately mitigated in RDS.

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?

Approved agencies and offices use the RDS client at outside of the post, and consequently have access to applicant PII. PII collected by those offices comes under the control of the post when I it has been accepted. A simple encryption is applied to the file that contains the RDS application (including PII) data on the software media used to transport the data between the off-site location and the Consulate. Access to RDS visa data and RDS server system at a post is limited to authorized DoS users (e.g., approving consular officer) with a need for RDS to perform their official duties. All authorized RDS server system users at post maintain a security clearance level at least commensurate with public trust positions. To access RDS at post, the authorized user must first be an authorized user of DoS' unclassified computer network then is issued a separate RDS user account and sign an access agreement describing the rules of behavior expected of the individual, including any prohibited activities (e.g., curiosity browsing). Access agreements are cleared by the post security officer. The level of access for an authorized user is based on least privilege. A system use notification ("warning banner") is displayed before log-on. Non-production uses (e.g., testing, training) of production data are strictly prohibited.

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

All authorized users must pass information security and privacy awareness training at least annually.

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.

Appropriate controls to limit access and to regulate the behavior of authorized users are fully implemented in RDS. Therefore this category of privacy risk is negligible.

11. Technologies

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

RDS does not employ technologies commonly considered to elevate privacy risk.

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

RDS does not employ technologies that elevate privacy risk.

12. Security

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

DoS operates RDS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. DoS has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. DoS performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, RDS was certified and accredited for 36 months to expire on October 31, 2009.