U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Remote Data Entry System (RDS)
October 2007

I. Describe the information to be collected (e.g., nature and source). Be sure to include any information in an identifiable form, e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc).

Remote Data Entry System (RDS) is used overseas to assist in the collection of non-immigrant visa (NIV) applicant data. RDS collects the information in an identifiable form, e.g., name, birth date of individual, gender, nationality, and place of birth.

II. Why is the information being collected (e.g., to determine eligibility)?

The RDS System is used overseas to assist in the collection of non-immigrant visa (NIV) applicant, petition and beneficiary data for visa applicants. This data is transmitted to the NIV system and database.

There are two application components: the RDS-Client and the RDS-Server applications. The RDS-Client application along with post issued barcode labels are distributed to remote user sites outside the consulates (travel agents and other semi-official businesses that collect NIV applicant data) by post staff to approved DOS remote user data entry sites.

The RDS-Client application is used by approved remote user sites to input applicant related NIV data. Posts also distribute ID barcode labels to approved remote user sites, allowing the sites to adhere a ID barcode label to the visa application. As a result, posts are able to quickly retrieve data once it is imported into both the RDS-Server and NIV applications.

The RDS-Client application provides the capability for the remote user sites to generate a data file or a delimited text file that is exported and automatically encrypted onto a diskette. The remote site sends the file, and, if applicable, the barcoded paper application forms and supporting documents to the post. The post then conducts a virus scan on the diskette before the data is imported into the RDS-Server application.

The RDS-Client application also has the capability to scan 2D barcodes generated from the electronic visa application forms (EVAF) system. The 2D barcodes include the applicant data entered directly into the EVAF online data entry form.
Some remote sites are equipped with 2D barcode generating software. The information is entered as a text file. The 2D barcode software then converts the text into a machine-readable barcode, allowing remote sites to scan the barcodes to enter applicant data in the

RDS-Client system.

Finally, the RDS-Client application has the capability to read the machine-readable zone (MRZ) which includes information from passports or visas. This information is used to populate fields in RDS-Client such as names and dates of birth.

The RDS-Server application allows post to enter applicant, petition, and beneficiary data for non-immigrant visas (NIVs). The RDS-Server application is also used by the posts to import and verify the data collected by the remote sites using the RDS-Client application. The RDS-Server application has the capability to scan 2D barcodes generated from the electronic visa application forms (EVAF) system. The 2D barcodes include the applicant data entered directly into the EVAF online data entry form.

Some remote sites are equipped with 2D barcode generating software. This software is used instead of the RDS-Client application for manual input. The information is entered as an unencrypted text file. Ultimately, the 2D barcode software converts the text into a machine-readable barcode as displayed below:

The RDS-Server can be considered a "front-end" data collection and transfer utility used by the posts to import and verify the data collected by the remote user sites, from the applicant's EVAF or existing passports and visas with MRZ. The RDS-Server then transmits the data to the NIV database in preparation for the issuance of visas.

The RDS-Server software interacts with Consular Shared Tables (CST) that maintains system login IDs and reference tables; and the RDS-Server software interacts with Consular Consolidated Database (CCD), which contains data replicated from all posts.

III. How will the information be used (e.g., to verify existing data)?

This is not applicable to RDS. RDS does not store data.

The RDS data, once collected, is transmitted to the Non-Immigrant Visa (NIV) system for processing. The RDS System does not store data. The RDS-Server application is considered a "front-end" data collection and transfer utility used by the posts to import and verify the data collected by the remote user sites.

IV. Will you share the information with others (e.g., another agency for a programmatic purpose)? If yes, list the entities.

No.

V. Describe what opportunities individuals have been given to decline to provide information or to consent to particular use of the information (e.g., whether individual may withhold permission for a particular use).

None

VI. How will the information be secured (e.g., administrative and technological controls)?

Access to RDS is limited to only authorized users. To ensure these users are valid, identification and authentication procedures are used. All users must be authenticated on the CA domains by logging on a workstation on the domain first. Once authenticated on the domain, the user must logon the RDS application which is installed locally on the workstation. Users must then identify and authenticate through the Consular Share Tables (CST) when accessing the RDS application. Each user is provided a unique identifier (userid) by a CST System Administrator. This user ID, which is created according to 12 FAM policies, is maintained by the CST system administrator, and complies with the following DoS userid format:

{Last name}{First initial}{Middle initial (if applicable)}

Incorporating the user's name into the userid allows for correlation between the user's activity on the system and his or her identity. The CST Administrator defines the CST user's role. This is accomplished within the CST application. Once defined within the CST application, all other CA application administrator that utilizes CST defines their user's roles within the CA applications that utilize CST. When it is determined that a user no longer needs access, the user account will be disabled.

Within the certified and accredited (C&A) boundary of RDS, only cleared technical personnel shall be allowed to access the components and no one shall be allowed to access the system until the appropriate background screening has been completed. This screening is conducted prior to the individual employment to provide a basis for ensuring his/her employment is clearly consistent with the interests of the National Security and all information system positions shall be designated in terms of sensitivity. Due to *privileged user* status the following administrators must restrict themselves from using their position to turn off/destroy audit trails, not to give unauthorized individuals privileged access, and modify the system to negate automated security mechanisms: System and Database Administrators.

RDS supports three user groups:

System Administrators/Users Security
Database Administrators
RDS end-users

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

RDS end-user access is determined based on their approved user role.

The ISSO, the system manager, and the end-user's supervisor structure access privileges to reflect the separation of key duties that end-user perform within the functions the application supports. Access privileges are consistent with the need-to-know, separation of duties, and supervisory requirements established for manual processes.

Once they are properly identified and authenticated by the system, the internal DoS user is authorized to perform all functions commensurate with the job requirements. In an effort to restrict users to only these required functions, logical access controls are utilized in accordance with the principle of least privilege and the concept of separation of duties. The specific RDS users' role must be identified by the user's manager requesting access for the identified user. RDS privileges relate directly to rights assigned to groups and user accounts associated with the directory services. A "right" authorizes a user to perform certain actions on the system and any user who logs on to an account to which the appropriate rights have been granted can carry out the corresponding actions. When a user does not have appropriate rights, the system blocks attempts to carry out those actions.

Once the user account has been created, the appropriate privileges are assigned to the user based on the requirements of their job functions, but limited to only the required privileges. This includes restricting the user's access to data files, peripherals, and their processing capability.

The RDS System Security Plan (SSP) documents the criteria, procedures, controls, and responsibilities regarding access.

VII. How will the data be retrieved (e.g., will it be retrieved by a personal identifier such as name, social security number, address, telephone number or some other identifier that is unique to an individual)?

This is not applicable to RDS. No information is stored by RDS.