U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Passport Record Imaging System Management (PRISM)
May 24, 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).

PRISM scans the passport application for digital archival and retrieval purposes. All of the applicant's personal information listed in the passport application is collected on the image form only. The passport application image can be viewed by authorized Department of State employees only.

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

To process and store full images of U.S. passport applications to include photographs. This image record will enable the Department to establish citizenship, identity, and entitlement to issuance of a U.S. passport.

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

PRISM was developed in order to perform and track the application images attached to each application for a U.S. passport.

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

PRISM data is **not** shared with any other Federal agency.

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).

The information solicited in the passport application is mandatory. The information solicited on the passport application is authorized by Titles 8, 22, and 26 of the United States Code, whether or not codified, including specifically 22 U.S.C. 211a et seq.; 26 U.S.C. 6039E, Section 236 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization

Act, Fiscal Years 2000 and 2001; Executive Order 11295 (August 5, 1966); and 22 CFR parts 50 and 51.

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

Information in PRISM has multi-level security which includes the PRISM application security, management controls (processes), technical controls (OpenNet security, access control lists) and Department physical site security. The Web access to PRISM data is based on management authorization and restricted to Department employees only.

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)?

Once PRISM data is stored in the database, the data is retrieved by other Department applications with read-only access. PRISM data is updated on the Passport Information Electronic Records System (PIERS) database using a unique PIERS identifier.