U.S. Department of State
Privacy Impact Assessment Summary

TITLE: Online Passport Status System (OPSS)
October 4, 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).

Information collected for OPSS comes directly from the applicant and includes the applicant’s last name, full date of birth and the last four digits of the applicant’s social security number.

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

The information is collected so passport applicants can check the status of their passport application.

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

The information is used to check passport application status.

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

The information in OPSS is not shared with other agencies.

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).

Passport applicants must acknowledge they have read the Department of State’s privacy and computer fraud and abuse acts notices and disclaimers before they are granted access to provide personal information to check on their passport application status. Applicants that choose not to acknowledge the notices and disclaimers are denied access to OPSS to check passport application status.

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

The OPSS is protected by technical, management and operational controls. Additionally, all user connections to the public web server are encrypted using a 128-bit SSL server certificate. The web server utilizes public key infrastructure (PKI) and requires a public key that matches the private key.

When the SSL public and private handshake is completed, the connection is encrypted and all data transmitted from either end is encrypted. Hence, individuals accessing the OPSS web site will not be permitted to add, change or delete data contained in OPSS.

If two or more records match the information entered by the applicant, no status is displayed and the applicant is asked to call the National Passport Information Center for their status.

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)?

Data is retrieved by entering a passport applicant's last name, date of birth and the last for digits of their social security number.