Privacy Impact Assessment
Of the
Passport and Visa System

Program or application name:

Passport and Visa System

System Owner:

Board of Governors of the Federal Reserve System's (Board) Office of the Secretary

Contact information:

System owner:	Angela Volcy
Title:	Passport Liaison
Organization:	Office of the Secretary (OSEC)
Phone:	202-452-3555
IT System Manager:	Sherrie Warren
Title:	Manager
Organization:	Information Technology (IT)
Phone:	202-736-5647

Description of the IT system:

The Passport and Visa System (PAVS) tracks and manages requests for official passports and/or travel visas by Federal Reserve System employees who are travelling on behalf of the Board or a Federal Reserve Bank, and the official passports and travel visas issued to those employees.

1. The information concerning individuals that is being collected and/or maintained:

The personally identifiable information collected and maintained in PAVS includes:

a. Name;
b. Date of Birth;
c. Employee Status (active/separated/retired);
d. Gender; and
e. Official Passport Number.

2. Source(s) of each category of information listed in item 1.

The personally identifiable information collected and maintained in PAVS is obtained from the Board's Fact Sheet for Foreign Travel and the application forms required by the U.S. State Department and relevant foreign country/countries completed by Federal Reserve System employees who request official passports and travel visas.

3. Purposes for which the information is being collected.

The Board's Office of the Secretary Clearing Section uses the personally identifiable information maintained in PAVS to process and track Federal Reserve System employee passport and travel visa requests with the U.S. Department of State and foreign embassies.

4. Who will have access to the information.

Access to the information collected and maintained in PAVS is generally limited to employees and contractors with the Board's Office of the Secretary Clearing Section who have a need for the information for official purposes. In addition, all information in the system may be disclosed for enforcement, statutory and regulatory purposes; to another agency or a Federal Reserve Bank; to a member of Congress; to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation; to contractors, agents, and others; and where security or confidentiality has been compromised to prevent, minimize, or remedy such harm that may occur.

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses.)

Individuals may elect not to submit the information into PAVS; however, that failure will result in the inability to obtain an official passport and/or travel visa for travel on behalf of the Board or a Federal Reserve Bank.

6. Procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date.

The personally identifiable information maintained in PAVS is obtained from Federal Reserve System employees requesting an official passport and/or travel visa for travel on behalf of the Board or a Federal Reserve Bank. Office of the Secretary Clearing Section staff does have the capability to update information if they become aware that an employee's information changes or is incorrect.

7. The length of time the data will be retained and how will it be purged.

Information in PAVS is retained for six years or longer, if needed for administrative or reference purposes. Electronic records are purged in accordance with established procedures.

8. The administrative and technological procedures used to secure the information against unauthorized access.

Access to PAVS is only granted to authorized users within the Office of the Secretary Clearing Section with a legitimate business need to use the information. Once a user has been approved, the system administrator is responsible for implementing the user's access to PAVS. Security logs are maintained to detect any unauthorized attempts at access. PAVS conforms to Federal Information Security Management Act and Board authentication requirements applicable to web applications. The system information is encrypted in the database to prevent unauthorized use. Moreover, IT Security scans application servers on a regular basis for viruses and malicious code. Finally, strict data validation controls and secure coding practices are used to protect the application from any attacks.

9. Whether a new system of records under the Privacy Act will be created. (If the data are retrieved by name, unique number or other identifier assigned to an individual, then a Privacy Act system of records may be created.)

The PAVS system is covered by an existing Privacy Act System of Records notice, entitled "FRB-Official General Files" (BGFRS-11). PAVS, therefore, does not require a new Privacy Act System of Records notice.

Reviewed:

Charles S. Struckmeyer */signed/*	07/23/2010
Chief Privacy Officer	Date
Maureen Hannan */signed/*	07/27/2010
Chief Information Officer	Date