I. What information is 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.

Passport Modernization System (PMS) investment is comprised of six major component systems, which together encompass passport processing at the integrated 'system' level: 1. Travel Document Issuance System (TDIS); 2. Passport Records Imaging Systems Management (PRISM) system; 3. Passport Information Electronic Records System (PIERS); 4. Passport Lookout Tracking System (PLOTS); 5. Front End Processor (FEP); and 6. External Front End Processor. It collects information in identifiable form as it relates to biographical, physical and demographic information on the individuals and the location the data was collected (e.g., document code, issue state, name, DOB, sex, date of expire, issuing authority).

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

The Passport Modernization program's objective is to modernize these systems providing direct support and service to the millions of U.S. citizens who each year apply for domestic passports to be used for travel abroad. This modernization includes increasing passport security and ensuring that applications for passports received from the public are processed and returned to the applicant in a timely manner.

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

The information maintained in the Passport Services records is used to establish the U.S. citizenship and identity of persons for a variety of legal purposes including, but not limited to the adjudication of passport applications and requests for related services, social security benefits, employment applications, estate settlements and federal and state law enforcement investigations.

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

Other systems sharing data or having access to Passport could be those that may be involved in national security; US border security, or federal law enforcement. Currently only lost/stolen passport data (to DHS) and overseas passport issuance data (to IRS to comply with Federal Tax law) is transferred to other agencies. The sharing of data and access for these transfers have been defined by memorandums of understanding (MOUs) between the affected agencies.
V. What opportunities do individuals have 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 applicant provides all data by completing forms. All forms at the time of data collection contain a Privacy Statement, which indicates what information is collected, why, for what purpose the information will be routinely used, who the information will be shared with and the consequences of not providing the data requested.

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

Access to data in Passport is determined based on the user’s role. A user role may allow access to all or only partial data in an applicant record. These accesses and roles are periodically reviewed by the system administrators to ensure a user does not have access to data for which they are not authorized to retrieve or view. Passport also trains its users on proper use of the system and on security awareness annually.

VII. Is a Privacy Act System of Records being created? (e.g., Will data 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)?

The corresponding System of Records notice for this system is Passport Records. STATE-26. Retrieval is based upon the individual’s name and/or passport application ID number.