Privacy Impact Assessment (PIA): Passport Records Imaging Systems Management (PRISM)

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: October 27, 2010

(b) Name of system: Passport Records Imaging Systems Management

(c) System acronym: PRISM

(d) IT Asset Baseline (ITAB) number: 896

(e) System description (Briefly describe scope, purpose, and major functions):

The Passport Records Imaging System Management (PRISM) manages archived images of passport applications for a United States passport. Used on-site at passport agencies, PRISM is a digital imaging system that scans and stores information in an easily retrievable format. The primary purpose of PRISM is to scan passport applications quickly, efficiently, and reliably and store these records for immediate access from any authorized Department PC terminal.

PRISM was developed in order to scan and track the application images attached to each application for a U. S. passport. Scanning is done only after the application has been completely processed, meaning that the passport must already have undergone adjudication, book printing and customer delivery. Scanned images of applications are maintained in PRISM for 100 years. The image information is also moved to the passport records archival database, Passport Information Electronic Records System (PIERS). The records need to be retained for 100 years due to the retention requirements of the original paper records. The records are used to verify citizenship, support residency requirements, help establish citizenship claims of descendents and conduct genealogical research. The National Archivist is considering their value as historical documents which would affect any determination of permanent retention.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): December 4, 2008

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

The initial source of data is provided by the individual applying for the U.S. passport. This information includes many elements of personal information. Passport applicant information maintained by PRISM is initially collected on any of the forms below submitted by the applicant.

- Form DS-11, used for first time passport applicants, requires the following information:
  - Name
  - Gender
  - Date and place of birth
  - Permanent mailing address
  - Telephone number
  - Social Security number
  - Passport and/or driver's license (or another type of identifying document number)
  - Photograph
  - Height
  - Eye color
  - Color photograph
  - Employer's name
  - Occupation
  - Marital status
  - Parents' names
  - Parents' date and place of birth
  - Whether parents are U.S. citizens
  - Emergency contact name
  - Emergency contact address
  - Emergency contact phone number
  - Emergency contact relationship to applicant
  - Dates and destinations of any planned travel

- Form DS-82 is for persons applying to replace a passport issued within the past 15 years who were over the age of 16 when the passport was issued, and who also provide the old passport with the application form. Form DS-82 requires the following information:
    - Name
    - Gender
    - Social Security number
    - Height
    - Hair color
    - Eye color
    - Occupation
    - Employer
    - Permanent mailing address
    - Email address
    - Telephone number
    - Date of trip
    - Length of trip
    - Countries to be visited
    - Emergency contact name
    - Emergency contact address
    - Emergency contact relationship to applicant

- Form DS-5504 is for persons replacing a passport that was issued less than a year earlier. The form may be used to replace an emergency passport with a fully valid one; to make a change to the applicant's identifying information (e.g., name change due to marriage or court order); or to correct a printing error in the passport. Form DS-5504 requires the following information:
    - Name
    - Date and place of birth
    - Social Security number
    - Gender
    - Height
    - Hair color
    - Eye color
    - Occupation
    - Employer
    - Contact information (where the passport should be mailed)
    - Permanent mailing address
    - Email address
    - Telephone number
    - Date of trip
    - Length of trip
    - Countries to be visited

- Form DS-4085 is used to add visa pages to a previously issued and currently valid passport. Form DS-4085 requires the following information:
  - Name
  - Date and place of birth
  - Social Security number
  - Permanent mailing address
  - Telephone number
  - E-mail address
  - Current passport number
  - Address on passport
  - Occupation
  - Employer
  - Emergency contact information
  - Date of trip
  - Length of trip
  - Countries to be visited

- Form DS-10 (birth affidavit) is used in conjunction with a Form DS-11 when an acceptable birth certificate cannot be obtained for a person born in the United States. Note that this form contains information about the applicant and the person making the affidavit (i.e., the affiant). Form DS-10 requires the following information:
  - Name
  - Gender
  - Date and place of birth
  - Permanent mailing address
  - Number of years the affiant has known the applicant
  - Relationship to the applicant or the basis of the affiant's knowledge regarding the applicant
  - Statement of all the facts known by the affiant about the applicant's birth
  - Signature of affiant
  - Permanent address of affiant
  - Identifying document submitted
  - Validation by Passport Agent, Acceptance Agent, or Notary Public

- Form DS-60 (affidavit regarding change of name) is used in conjunction with a Form DS-11 when the name which is used by the applicant (1) is substantially different from that shown on the evidence of citizenship, or (2) has been adopted without formal court proceedings and was not acquired by marriage. Note that this form contains information about the applicant and the person making the affidavit. Form DS-60 requires the following information:
  - Current name of applicant

  - Approximate date current name was assumed
  - Number of years the affiant has known the applicant
  - Former name of applicant
  - Applicant's date and place of birth
  - Number of years the affiant has known the applicant
  - Relationship to the applicant
  - Printed name of affiant
  - Permanent address of affiant
  - Identifying document submitted
  - Validation by Passport Agent, Acceptance Agent, or Notary Public

- Form DS-64 is used in conjunction with a Form DS-11 when a previous valid or potentially valid U.S. passport cannot be presented. Form DS-64 requires the following information:
  - Name
  - Gender
  - Date and place of birth
  - Social Security number
  - Telephone numbers
  - E-mail address
  - List of lost or stolen passport numbers
  - List of dates that lost or stolen passports were issued
  - Information on how, where, and date when the loss or theft took place
  - If lost, efforts that were taken to recover the passport

- Form DS-71 is used in conjunction with a Form DS-11 only when the applicant for a passport is unable to establish his or her identity to the satisfaction of a person authorized to accept passport applications. Form DS-71 requires the following information:
  - Passport applicant name
  - Relationship to the applicant
  - Length of time the witness has known the applicant
  - Witness name
  - Witness permanent address
  - Witness date and place of birth
  - Witness telephone number
  - Information on whether the witness has been issued a U.S. passport
  - Witness passport number
  - Place of issue of witness passport (if possible)
  - Date of issue
  - Witness signature and date

- Form DS-86 is used when the passport applicant does not receive the U.S. passport card and/or passport book for which he or she applied. Form DS-86 requires the following information:

  - Name
  - Date of birth
  - Contact telephone numbers
  - Permanent address
  - Where the previous application was filed
  - Signature and date

- Form DS-3053 is used in conjunction with a Form DS-11 if a non-applying parent or guardian consents to the issuance of a passport for his or her minor child who is younger than 16 years old. Form DS-3053 requires the following information:
  - Minor's name
  - Minor's date of birth
  - Relationship to minor
  - Statement of consent
  - Statement of consent notarization
  - Statement of special circumstances

The above forms may be completed by the applicant on published paper forms available at many government office locations or may be completed online using web forms at the U.S. Department of State's public web site, www.travel.state.gov. If web forms are used, the applicant must still print the form and submit it as a hardcopy with supporting documents to the mailing address indicated on the form, in person at a domestic passport office, or at a United States embassy or consulate.

b. How is the information collected?

Information is collected directly from the applicant using one or more of the above forms. The PRISM system operates in three stages: application handling/documentation preparation; scanning; and quality control/archival. During the first stage, approximately 60 to 90 days after applications are completed or abandoned, they are scanned locally at the agency. Alternatively, they are boxed and shipped to the Records Management Branch of the Information Management Liaison Division (CA/PPT/IML/R). The boxes are received by the CA/PPT/IML/R staff, and then queued for scanning and archival by PRISM. The scanning stage includes the unbinding of documents, clearing any folds within the forms, and removing any miscellaneous debris from the package. Forms are then scanned into PRISM using high-speed Imaging Business Machines, LLC (IBML) scanners. The scans capture a full image of the top of the application, which includes the application data and photograph. The IBML scanner collates the pages to ensure that all passport application records are kept in the same order in which they were received. Finally, in the quality control/archival stage, the original physical forms are re-boxed, and all scanned images are reviewed through a comprehensive quality control process. Scanned images are examined for color, data accuracy, and readability.

c. Why is the information collected and maintained?

PRISM is used to scan passport applications quickly, efficiently, and reliably and to store these records for immediate access from any authorized PC terminal. PRISM is also used to populate PIERS (Passport Information Electronic Records System). PIERS is then used to provide authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously processed passport applications and vital record data for the purpose of adjudicating passport applications, and confirming citizenship and eligibility of persons to receive other consular services.

d. How will the information be checked for accuracy?

Accuracy of the information on a passport application and submission of citizenship evidence is the responsibility of the passport applicant. Quality checks are conducted against the submitted documentation at every stage, and administrative policies are established to minimize instances of inaccurate data.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 USC Sec. 211a-218, Electronic Passport Application Form Web Site
- 26 USC 6039E, Information Concerning Resident Status
- Section 236 of the Admiral James W. Nance and Meg Donovan Foreign Relations Authorization Act, Fiscal Years 2000 and 2001
- Executive Order 11295, Rules Governing the Granting, Issuing, and Verifying of United States Passports, August 5, 1996
- 22 C.F.R. parts 50 and 51, Citizenship and Naturalization and Passports and Visas

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The personal data collected by PRISM is the minimum necessary to carry out the function of PRISM as identified in Section 3c above. The primary privacy risk is:

- **Insider threat** – employee misuse of data.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety

Numerous management, operational, and technical security controls are in place to protect the data, in accordance with the Federal Information Security Management

Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). These controls include regular security assessments, physical and environmental protection, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewall, intrusion detection systems, and antivirus software), training, and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The primary use of PRISM is for Department of State employees authorized to use the system to have quick, efficient, and reliable computer access to the scanned images of passport applications throughout the passport issuance process for the purpose of adjudicating passport applications and confirming citizenship and eligibility of persons to receive other consular services. PRISM data also serves an archival purpose as part of PIERS.

b. What types of methods are used to analyze the data? What new information may be produced?

Hi-resolution images stored in PRISM are used for the Facial Recognition feature in TDIS.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

No commercial information, publicly available information, or information from other Federal agency databases is used in PRISM. All of the information in PRISM is derived from completed U.S. passport applications.

d. Are contractors involved in the uses of the PII?

PRISM is a government owned system that utilizes government off the shelf software (GOTS) and is developed, maintained and supported by contractors. All users were required to pass annual computer security/privacy awareness training, and to sign non-disclosure and rules of behavior agreements.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

PRISM is a government system. It is supported by contract employees, who support U.S. government employees in their maintenance of the system.

Contractors who support PRISM are subjected to a background investigation by the contract employer equivalent to a “National Agency Check” of the files of certain U.S. Government agencies (e.g., criminal law enforcement and Department of Homeland Security databases) for pertinent facts bearing on the loyalty and trustworthiness of the individual. Contractors involved in the development or

maintenance of PRISM hardware or software must have at least a Secret-level security clearance.

All employees and contractors undergo an annual computer security briefing and Privacy Act briefing from both the Department of State and the contract employer. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

5. Retention

a. How long is information retained?

The established retention period for electronic records in PRISM is presently 100 years in accordance with published record schedules as approved by the National Archives and Records Administration (NARA). The following record schedule specifies that these records are to be destroyed when they are 100 years old: Chapter 13 Passport Records A-13-001-01c(2)(a) DispAuthNo: NCI-59-79-12 item 1b – Transfer to WNRC monthly.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely that inaccuracies will develop as a consequence of aging.

Regular backups are performed and recovery procedures are in place for PRISM. All records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached the end of their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration's disposition schedules.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

PRISM is used to populate PIERS (Passport Information Electronic Records System), which is used to provide authorized users at domestic passport agencies and overseas posts with the ability to query information pertaining to previously processed passport applications and vital record data for the purpose of adjudicating passport applications, and for confirming citizenship and eligibility of persons to receive other consular services.

The Bureau of Consular Affairs oversees a network of facilities that may internally share or disclose the personal information collected and maintained in PRISM to personnel with a "need-to-know". These facilities include over a dozen regional passport agencies, a special issuance agency, three national processing facilities, the National Passport Information Center, and the Headquarters offices in Washington, DC. The information may also be shared in a law enforcement inquiry, and/or in an emergency situation subject to the provisions of the Privacy Act.

The information shared is the information listed on the application regarding the individual and adjudication notes made by the passport examiner. PRISM redacts the name of the reviewing official.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

The risks associated with sharing privacy information internally and the disclosure of privacy information is generally associated with personnel. Intentional and unintentional disclosure of personal information from personnel can result from social engineering, phishing, abuse of elevated privileges or general lack of training. To combat the misuse of information by personnel, there are numerous management, operational and technical controls in place to reduce and mitigate the risks associated with internal sharing and disclosure including, but not limited to, annual security training, separation of duties, least privilege, personnel screening, and auditing.

Vulnerabilities and risks are also mitigated through the system's certification process. NIST recommendations are followed to ensure hardening of all data transfers and storage is applied.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

PRISM does not interface with external entities. Persons or government agencies external to the Department of State's OpenNet are not able to connect to PRISM.

However, PRISM does provide data to PIERS, which shares information with numerous external organizations. PIERS may share passport information with any of the following organizations: (1) the Department of Homeland Security (DHS) for border patrol screening and security purposes, law enforcement, counterterrorism, and fraud prevention activities; (2) the Department of Justice (DOJ) bureaus,

including the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the U.S. Marshals Service for law enforcement, counterterrorism, border security, fraud prevention, and criminal and civil litigation activities; (3) the Internal Revenue Service (IRS) to obtain the current addresses of specifically identified taxpayers in connection with pending actions to collect taxes accrued, examinations, and/or other related tax activities; (4) the National Counterterrorism Center (NCC) to support strategic operational planning and counterterrorism intelligence activities; (5) the Office of Personnel Management (OPM), other federal agencies, or contracted outside entities to support investigations for OPM, other federal agencies, and to aid contractor personnel conducting investigations prior to issuance of security clearances; (6) Federal, state, local, other agencies for use in legal proceedings as government counsel deems appropriate, in accordance with any understanding reached by the agency with the U.S. Department of State; (7) Assistance to parents of underage minors (in support of the mission of the Bureau of Consular Affairs, Office of Children's Issues in the context of abductions that occur overseas); (8) Upon request of attorneys representing an individual in administrative or judicial passport proceedings when the individual to whom the information pertains is the client of the attorney making the request; (9) Members of Congress when the information is requested on behalf of or at the request of the individual to whom the record pertains; (10) Foreign governments, to permit such governments to fulfill passport control and immigration duties and their own law enforcement, counterterrorism, and fraud prevention functions in support of U.S. law enforcement, counterterrorist, and fraud prevention activities; and (11) Government agencies other than the ones listed above that have statutory or other lawful authority to receive such information on a need-to-know basis and subject to the provisions of the Privacy Act.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

External organizations do not have access to PRISM. Any sharing outside the Department is done through PIERS.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

N/A

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable system of records:

STATE 26: Passport Systems

☐ does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Yes. Individuals are made aware of the uses of the information on the forms used to collect it identified in Section 3(a) above. Each published form associated with PRISM contains a Privacy Act statement in conformance with the requirements of the Act. Each form (including online web forms) exhibits an OMB authorization number indicating it is an approved information collection. The website that provides applicants the ability to complete an electronic application contains a tailored website privacy policy that describes the terms of use of the personal information provided.

Notice is also published in the System of Records Notice (SORN) titled STATE-26, Passport Systems. By providing the information requested at the initial request for passport or passport renewal, processing and issuance of the passport, U.S. citizens are consenting to the use of the information for its identified purpose.

b. Do individuals have the opportunity and/or right to decline to provide information?

An application for a passport is a voluntary action by a record subject. With the exception of his or her Social Security Number, an applicant is not legally required to provide the information requested on the passport application form. However, failure to do so may result in either Passport Services' refusal to accept the application or in the denial of a U.S. passport.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. No other special uses of the information are permitted. Users are advised on the use of the information being collected. This process has occurred during the first-time passport request or passport renewal request, payment and issuance. The data stored in the PRISM system is stored permanently after issuance of the passport.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

Notice is given to individuals as described in Section 8(a) above. The notice offered is reasonable and adequate in relation to the system’s purposes and uses.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

PRISM contains Privacy Act-covered records; therefore, notification and redress are rights of record subjects. Procedures for notification and redress are published in the system of records notice identified in section 8 above, and in rules published at 22 CFR 171.31. The procedures inform individuals about how to inquire about the existence of records about themselves, how to request access to their records, and how to request amendment of their records. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of passport records on grounds pertaining to law enforcement. These exemptions are in the interest of national defense and foreign policy, if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. They are published as agency rules at 22 CFR 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose and uses.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to PRISM is limited to authorized Department of State employees/contractors in the performance of their official duties. All such authorized government users are required to maintain a security clearance level commensurate with their position. To gain authorized access to the Department network and to the system, the employee/contractor must pass mandatory cybersecurity and privacy awareness training.

The system restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel. The level of access for the user restricts the data that may be viewed. In all situations a system use notification ("warning banner") is displayed before log-on is permitted and recaps the restrictions on the use of the system. All activity by every authorized user is monitored, logged, and audited.

Non-production uses (e.g., testing, training) of production data are restricted by administrative controls.

The internal interface between PRISM and other systems is monitored and guided by the security controls on OpenNet. Controls built into OpenNet, including routers and the Network Intrusion Detection System (NIDS), provide network level controls designed to mitigate the risk of unauthorized access. Other internal systems that

interface with PRISM are strictly controlled by routers and NIDS rules that set strict limits to the PRISM system.

Additionally, a variety of configuration auditing and vulnerability scanning tools and techniques periodically monitor OpenNet-connected systems including PRISM.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to undergo computer security and privacy awareness training prior to accessing the system and must complete refresher training yearly in order to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Several steps are taken to reduce residual risk related to system and information access. Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly terminated. Additionally, the system audit trails that are automatically generated are regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed—or attempted to perform—on an information system.)

11. Technologies

a. What technologies are used in the system that involve privacy risk?

PRISM operates under standard, commercially-available software products residing on a government-operated computing platform not shared by other external business applications or technologies. No technologies that are known to elevate privacy risk are employed in PRISM.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No technologies that are known to elevate privacy risk are employed in PRISM.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates PRISM in accordance with information security system requirements and procedures required by federal law and policy to ensure that information is appropriately secured. The Department has conducted a risk assessment of the system, identified appropriate security controls to protect against that risk, and implemented those controls. The Department performs monitoring, testing, and evaluation of security controls on a regular basis to ensure that the

controls continue to work properly. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, its most recent date of authorization to operate (ATO) was February 27, 2008.