Passport Records Imaging Systems Management (PRISM)

1. Contact Information

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

2. System Information

(a) Date PIA was completed: December 4, 2008

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

(c) System acronym: PRISM

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

(e) System description:

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 PC terminal.

PRISM was developed in order to perform and track the application images attached to each application for a United States 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 up to 60 days, at which time the information is moved to the passport records archival database, PIERS (Passport Information Electronic Records System).

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification

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

(h) Date of previous PIA (if applicable): February 11, 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 a host of personal information. Examples of personal information collected include:

- Name
- Date and place of birth
- Address
- Telephone number
- Social security number,
- Passport and/or Driver's license (or another type of identifying document number)
- photograph

Passport applicant information maintained by PRISM is initially collected on any of these forms submitted by the applicant:

- Form DS-11 is used for passport applications from first time applicants.
- Form DS-82 is for persons applying to replace a passport issued within the past 15 years, who are over the age of 16 when the passport was issued, and who also provide the old passport with the application form.
- 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 full validity 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 their passport.
- Form DS-4085 is used to add visa pages to a previously issued and currently valid passport.
- Form DS-10 is used in conjunction with a DS-11 when an acceptable birth certificate cannot be obtained for a person born in the United States.
- Form DS-60 is used in conjunction with a DS-11 when the name which is used by the applicant is (1) 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.
- Form DS-64 is used in conjunction with a DS-11 when a previous valid or potentially valid U.S. passport cannot be presented.
- Form DS-71 is used in conjunction with a 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-86 is used when passport applicant does not receive the U.S. passport card and/or passport book for which he or she applied.
- Form DS-3053 is used in conjunction with a DS-11 if a non-applying parent or guardian consents to the issuance of a passport for his or her minor child that is younger than 16 years old.

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 Department of State's public web site. If web forms are used, the applicant must still print the form and submit it as hardcopy with supporting documents.

b. How is the information collected?

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 boxed and shipped to the Records Management Branch of the Information Management Liaison Division. The boxes are received by the IML/R staff, 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 IBML scanners. The scans capture a full image of the top of the application, which includes application data and photograph. The IBML scanner collates the pages to ensure that all applications 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's purpose is two-fold. The primary purpose of PRISM is to scan passport applications quickly, efficiently, and reliably and store these records for immediate access from any authorized PC terminal. Second, 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.

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.

Once the data is scanned, PRISM has a Quality Control/Archival feature. Scanned images are reviewed through a comprehensive quality control process that examines color, view-ability and image accuracy. Applications can be rescanned if necessary. Once scanned, images are archived to an optical Write-Once/Read-Many (WORM) drive.

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

- 22 USC Sec. 211a-218 ("The Secretary of State may grant and issue passports, and cause passports to be granted, issued, and verified in foreign countries by diplomatic and consular officers of the United States, and by such other employees of the Department of State who are citizens of the United States as the Secretary of State may designate, and by the chief or other executive officer of the insular possessions of the United States, under such rules as the President shall designate and prescribe for and on behalf of the United States, and no other person shall grant, issue, or verify such passports.")
- 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)

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

There are numerous management, operational, and technical security controls in place to protect the data, in accordance with the Federal Information Security Management Act of 2002 and the information assurance standards published by the National Institute of Standards and Technology. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), 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 to have quick, efficient, and reliable computer access to the scanned images of passport applications associated throughout the passport issuance process. 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?

The archived images are not used for analytical purposes nor are they intended to produce new information.

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. Is the system a contractor used and owned system?

PRISM is a government owned system that utilizes government off the shelf software (GOTS) and is developed, maintained and supported by contractors.

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 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 of the Department of State and as approved by the National Archives and Records Administration.

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

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 their retention period, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA).

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 shared with personnel with a need to know within the Department. 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. The information may be shared to assist in a law enforcement inquiry, and/or in an emergency situation.

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.

Vulnerabilities and risk are mitigated through the system's certification process. NIST recommendations are followed to ensure hardening of all data transfers and storage is applied. Residual risk is then accepted through the authorization process.

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 with numerous external organizations. PIERS may share passport information with any of the following organizations: (1) Department of Homeland Security for border patrol, screening, and

security purposes; law enforcement, counterterrorism, and fraud prevention activities; (2) Department of Justice, including the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Marshals Service, and other components, for law enforcement, counterterrorism, border security, fraud prevention, and criminal and civil litigation activities; (3) Internal Revenue Service for the current addresses of specifically identified taxpayers in connection with pending actions to collect taxes accrued, examinations, and/or other related tax activities; (4) National Counterterrorism Center to support strategic operational planning and counterterrorism intelligence activities; (5) Office of Personnel Management (OPM), other federal agencies, or contracted outside entities to support the investigations OPM, other federal agencies, and contractor personnel conduct for the federal government in connection with verification of employment eligibility and/or the issuance of a security clearance; (6) Federal, state, local or 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; (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, and to support U.S. law enforcement, counterterrorism, 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.

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.

Vulnerabilities and risk are mitigated through the system's certification process. NIST recommendations are followed to ensure hardening of all data transfers and storage is applied. Residual risk is then accepted through the authorization process.

8. Notice

The system:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

Passport Records–STATE–26

Overseas Citizens Services–STATE–05

☐ does NOT contain information covered by the Privacy Act.

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

Individuals are made aware of the uses of the information prior to the collection. Notice is also published in the System of Records Notice 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 for the information to be used for its identified purpose.

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

With the exception of their 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 Passport Services' refusal to accept the application or result 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 passport or passport renewal request, payment and issuance. The data store in the PRISM systems is stored 60 days 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.

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 paragraph 8 above, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about the existence of records about them, how to request access to their records, and how to request amendment of their record. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of a passport records on grounds pertaining to law enforcement, 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. These exemptions 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 the Department network and to the system, the employee/contractor must pass mandatory cyber security 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 of the OpenNet. Controls built into the 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 router 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 platforms 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.

N/A - 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 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 provision for the triennial recertification of this system, its most recent date of authorization to operate was February 27, 2008.