PRIVACY IMPACT ASSESSMENT

Passport Application Management System (PAMS) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Name of system: Passport Application Management System
(b) Bureau: Consular Affairs
(c) System acronym: PAMS
(d) iMatrix Asset ID Number: PAMS #120521 (MIS 724, PDITS 5227, PIERS 85, PLOTS 346, UMWS 4377)

(e) Reason for performing PIA: Click here to enter text.
   ☐ New system
   ☐ Significant modification to an existing system
   ☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): Click here to enter text.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?
   ☒ Yes
   ☐ No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?
   The system received an Extension of Authorization to Operate (ATO) on May 8, 2017. The authorization is valid until rescinded or the expiry date of July 31, 2019.

(c) Describe the purpose of the system:
   PAMS is a logical business grouping of all passport applications for the Bureau of Consular Affairs (CA), which consists of Management Information System (MIS), Passport Data Information Transfer System (PDITS), Passport Information Electronic Records System (PIERS), Passport Lookout Tracking System (PLOTS), and User Manager Web Security (UMWS).

   MIS
   The Management Information System (MIS) is a web-based reporting tool that tracks predefined productivity statistics of U.S. passport agencies. It provides passport system
management the ability to query the Travel Document Issuance System (TDIS) databases for information specific to any passport agency within the United States. This information includes weekly and monthly workloads, book inventory, agency hiring summaries, and statistics regarding agency staff.

**PDITS**
The Passport Data Information Transfer System (PDITS) is a consolidation of database functionality and support under one design, development, and management structure. PDITS interfaces with TDIS and Online Passport Status Service Structured Query Language (OPSS SQL). Prominent associations include being the recipient and repository of all issued passport data from TDIS. PDITS's mandate is to continually ensure data quality and integrity in the passport databases, particularly with respect to the data imported from TDIS.

**PIERS**
The Passport Information Electronic Records System (PIERS) is a suite of web and desktop applications that provide query and management capabilities for passport records, Consular Reports of Birth Abroad (CRBAs), Certificates of Witness to Marriage (CWM), Records of Death (ROD), Advance Finder (AF), Diplomatic and Official Tracking System (DOTS), and Panama Canal Zone (PCZ) data. It operates on the Department of State’s OpenNet network. (The OpenNet network is the Department of State’s internal network or intranet.) PIERS provides direct access for OpenNet users at passport agencies, posts abroad, Department of State directorates and offices and Record Services, and indirect access for external users through the Consular Consolidated Database (CCD).

The PIERS system provides users with both case-based and user-based views of information and support for electronic checking and reporting of work processes. Case-based views refer to the different types of data records that the PIERS system and database maintain. This includes passport information (all records of issued and expired passports, not issued applications, and destroyed/stolen/lost passports) and consular records of overseas births and deaths. User-based views refer to the PIERS systems ability to provide access to different data elements, record types, and system functions based on specific groups or system application roles assigned to individual users.

**PLOTS**
The Passport Lookout Tracking System (PLOTS) is a web enabled case management and image archive system used to manage and adjudicate Consular Lookout Automated Support System (CLASS) cases. The purpose of the PLOTS application is to provide CA domestic and post users with an efficient and reliable solution to the recording, managing, searching and process streamlining of CLASS cases.

**UMWS**
User Manager Web Security is a web-based application used to manage user accounts. User Manager Web Security (UMWS) allows users to be assigned privileges to access Passport systems to perform their tasks. User accounts for Bureau of Consular Affairs personnel who are authorized to access the Passport Information Electronic Records System (PIERS), Management Information System (MIS), Passport Records Imaging System Management (PRISM), and Passport Lookout Tracking System (PLOTS) are created and assigned the appropriate privileges in UMWS. The user then can perform the tasks associated with the privileges.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

PAMS
- Names of Individuals
- Birthdates of Individuals
- Social Security Number or other Identifying Number
- Phone Number(s) of Individuals
- Business Addresses
- Personal Addresses
- Email Addresses of Individuals
- Images or Biometrics Identifiers

MIS
The Passport Services Directorate of the Department of State (CA/PPT) uses the web-based Management Information System (MIS) to collect data and compile statistics related to the passport processing activities of passport agencies. Departmental users collect data, compile statistics and report on the following:
- passport production/ workload
- labor and staffing statistics
- passport employee productivity
- fees collected
- product inventory
- PLOTS case tracking
- PIERS privacy and user activity

MIS retrieves the data from a variety of departmental databases and permits the user to schedule and run reports based on system privileges. MIS does not contain or report PII of passport requesters but merely permits departmental users to aggregate the statistics regarding passports requested, issued/denied, due dates and similar information.

PDITS
PDITS receives the following PII as a data transfer from TDIS. TDIS obtains the information from passport books and passport cards, applications for passport books and passport cards, amendments, extensions, replacements, and/or renewals of passport books or cards. The information is not directly collected from the applicant. Although the DS 4085 is no longer accepted for additional visa pages, the form is in the system and used for other purposes such as miscellaneous actions, and collects the same PII.

- applicant's name
- date of birth
- place of birth
- gender
- Social Security number
- biometric IDs
- legal and family information
- mailing address
- email address

PIERS

PIERS collects the following PII elements:

- name
- date of birth
- address
- telephone number
- Social Security number
- passport number
- driver’s license or other identifying number(s)
- education information
- financial transactions
- employer
- medical information

The passport applicant provides the information via web-based PIERS. The PIERS data is input into TDIS and transferred via the Front End Processor (FEP), which communicates with PIERS to create new records and modify the records, and data share, which feeds data to PIERS. The data includes an approved passport application from the Post repository server, which is in place for the sole purpose of supplying OPSS with passport status data.

PLOTS

PLOTS collects and maintains records related to applications for U.S. passports and loss of
nationality. Sources of the information are U.S. citizens applying for passports, other Department of State computer systems, passport specialists, and fraud prevention managers. The record subjects in PLOTS are past and current applicants for a U.S. passport who may be suspected of having felony warrants, suspected of committing passport fraud, owe debts to dependents, be indebted to the federal government for a repatriation or other loan, or may be denied a passport or be issued only a restricted passport for certain other reasons permissible by statute and/or regulation.

Components of an individual's record (called a "case") in PLOTS are of two kinds. The first kind is the passport application and all supporting documentation related to it, including citizenship evidence, correspondence, reports of investigation, passport specialists’ diary entries, court orders, passport revocation actions, and passport denial actions. (For a detailed description of PII in passport applications, please see the TDIS PIA.) The passport application and supporting documents are imported into PLOTS electronically by way of separate Consular Affairs passport processing systems, not directly from the applicant. The second kind of information in PLOTS about an individual is one or more "lookouts." Lookouts serve to alert passport specialists of possible fraud or other irregularities related to a person having the same or similar name and date of birth as that of the applicant. Lookouts are created by passport specialists at passport agencies/centers and at overseas posts in PLOTS which are then entered into the Consular Lookout and Support System (CLASS).

**UMWS**

UMWS collects last name, first name, login ID, office location, office phone number, office email address of federal employees who access applications in PAMS.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure)
- 22 U.S.C. 211a-218, 2705 (Passports and Consular Reports of Birth Abroad)
- 22 U.S.C 2651a (Organization of Department of State)
- Executive Order 11295, of August 5, 1966, 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1185 (Travel Documentation of Aliens and Citizens)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)? ☒ Yes, provide:
- SORN Name and Number:
  STATE-26 - Passport Records, March 24, 2015
  STATE-05 - Overseas Citizens Records, September 8, 2016

☐ No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐ Yes ☒ No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒ Yes ☐ No

(If uncertain about this question, please contact the Department’s Records Officer at records@state.gov.)

If yes provide:
- Schedule number, Length of time the information is retained in the system, and Type of information retained in the system:
  A-13-001-02 Passport Books: Recovered, Surrendered, Unclaimed or Found
  Description: These passports books were issued to individuals who have returned them on their own initiative or at the request of the Department of State or other Government agency or have been found, recovered, and/or forwarded to Passport Services (PPT/TO/RS). They include Diplomatic or other official passports issued to military personnel who are either discharged, retired or deceased during the validity period of the passport; No Fee passports issued to Peace Corps volunteers; tourist passports; and all other passports.
  Disposition: Destroy after receipt has been logged into PIERS database or successor electronic database. (ref. N1-059-96-5, item 2)
  DispAuthNo: N1-059-04-2, item 2

  A-13-001-16 Passport Lookout Master
  Description: This online information system assists Passport Services staff in determining those individuals to whom a passport should be issued or denied, identifies those individuals who have been denied passports, or those who are not entitled to the issuance of full validity passport and those whose existing files must be reviewed prior to issuance.
  Disposition: Destroy when active agency use ceases. (ref. N1-059-96-5, item 16)
  DispAuthNo: N1-059-04-2, item 16

  A-13-002-02 Requests for Passports
**Description:** Copies of documents relating to selected passport requests.

**Disposition:** Temporary: Cut off at end of calendar year. Hold in current file area and retire to Records Service Center when 2 years old. Destroy/delete when twenty-five (25) years old.

**DispAuthNo:** N1-059-05-11, item 2

**A-13-002-03 Tracking/Issuance System**

Description: Electronic database used for maintenance and control of selected duplicate passport information/documentation.

Disposition: Permanent: Delete when twenty-five (25) years old.

**DispAuthNo:** N1-059-05-11, item 3

### 4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public
☒ U.S. Government employees/Contractor employees
☐ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒ Yes  ☐ No

- If yes, under what authorization?
  26 U.S.C. 6039E (Information Concerning Resident Status) and
  22 U.S.C. § 2714a. (f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(c) How is the information collected?

The passport information is collected when an applicant fills out an application for a passport and/or passport card or other passport services offered. The following forms apply:

- Department of State Form (DS 11) – Application for a U.S. Passport (First-time applicants, all minors, and applicants who are not eligible to use the DS 82)
- Department of State Form (DS 82) – U.S. Passport Renewal Application for Eligible Individuals (by mail)
- Department of State Form (DS 5504) – Application for a U.S. Passport (Corrections, Name Change within 1 year of Passport issuance)
- Department of State Form (DS 64) – Statement Regarding Lost or Stolen Passport
- Department of State Form (DS 3053) – Statement of Consent – Issuance of a Passport to a Minor Under Age 16
- Department of State Form (DS 5525) – Statement of Exigent/Special Family Circumstances – For Issuance of a Passport to a Minor Under Age 16
- Department of State Form (DS 86) – Statement of Non-Receipt of a U.S. Passport
(d) Where is the information housed?
- ☒ Department-owned equipment
- ☐ FEDRAMP-certified cloud
- ☐ Other Federal agency equipment or cloud
- ☐ Other
  - If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?
The accuracy of the information is checked against sources including but not limited to, Social Security Administration, Law Enforcement, and Internal Revenue Service.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?
Passport applicants are responsible for providing current information on their passport applications. Passport applicants can modify or amend records by accessing the website where the record was established or by contacting the relevant departmental office. Information can also be updated during the adjudication process. Information in PAMS is updated when an applicant submits a passport application. The information is only as current as the last update to the data specific to PAMS and PAMS components.

(g) Does the system use information from commercial sources? Is the information publicly available?
The system does not get information from commercial sources nor is it publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?
Yes, a passport applicant is advised of all the relevant privacy implications at the time the individual completes and signs the application via a Privacy Act Statement. The applicant is notified of the following:
- His/her PII is being collected
- The purpose for which it is required
- The possible uses of the information
- The possibility that the data may be shared with other organizations/agencies
- How the data is protected from unauthorized/illicit disclosure
- Potential consequences if the applicant declines to provide the data (e.g. that his/her passport application may be declined).

Completing, signing and submitting a passport application serves as legal consent from the individual to authorize the U.S. government to utilize his/her information for specific purposes, to include adjudicating his/her passport application, and under certain circumstances to revoke the passport in accordance with U.S. law.
(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☒Yes ☐No

- If yes, how do individuals grant consent?
At the time applicants complete the passport application, they are notified of their option to decline to provide the required information, and they are advised that to do so may cause their passport application to be denied. Passport applicants are also notified of the relevant privacy implications of providing their information, and how their information may be used and shared with other agencies. Passport applicants are not given the option to selectively consent to or deny specific uses of the information. The passport applicant grants complete consent upon signing the application. The applicant’s signature provides the authorization to the U.S. government to use and share the information.

- If no, why are individuals not allowed to provide consent?

(j) How did privacy concerns influence the determination of what information would be collected by the system?
The Department of State understands the need for PII to be protected. Accordingly, the PII in PAMS is handled in accordance with federal privacy regulations regarding the collection, access, disclosure, and storage of PII. PAMS only collects the information necessary for the processing of passport applications.

5. Use of information

(a) What is/are the intended use(s) for the information?
PAMS is a logical business grouping of all passport applications for CA, which consists of Management Information System (MIS), Passport Data Information Transfer System (PDITS), Passport Information Electronic Records System (PIERS), Passport Lookout Tracking System (PLOTS) and User Manager Web Security (UMWS).

MIS
Passport Agencies and the Department of State headquarters use the MIS system, a web-based application, to collect data on:

- Passport production – the production data is submitted both weekly and monthly
- Labor & Staffing – the staffing data is submitted weekly

PDITS
PDITS receives PII (passport books and passport cards, applications for passport books and passport cards, amendments, extensions, replacements, and/or renewals of passport books or cards) from TDIS to electronically verify and validate PII. This information is shared with
the Department of Homeland Security/Customs and Border Protection (DHS/CBP) to validate and authorize admissions and exits of persons in the U.S.

PIERS

The PIERS system provides its users with both case-based and user-based views of information, and support for electronic checking and reporting of work processes. Case-based views of information are used to manage and track record access cases for issued passports, providing information such as reasons for adjudication decisions for use in processing passports. Such information includes all records of issued and expired passports, not issued applications, destroyed/stolen/lost passports and consular records of overseas births. User-based views of information assist the PIERS system in determining access to different data elements, record types, and system functions based on specific groups or system application roles assigned to individual users.

PLOTS

PLOTS is used by the Bureau of Consular Affairs Directorate of Passport Services, other Consular Affairs offices, and the Bureau of Diplomatic Security. Information contained in PLOTS allows these users to manage and track a passport lookout case. Lookouts are created by passport specialists at passport agencies/centers and at overseas posts in PLOTS. Lookouts data alerts passport specialists of possible fraud or other irregularities related to a person having the same or similar name and date of birth as that of the applicant. PLOTS information assists in determining a potential denial of a passport, initiation of a criminal investigation, fraud and fraud prevention, a child in the Children’s Passport Alert Program or issues related to verifying the applicant’s citizenship or identity.

UMWS

The information in User Manager Web Security (UMWS) is used to assign access to Passport systems. User accounts for Bureau of Consular Affairs personnel who are authorized to access the Passport Information Electronic Records System (PIERS), Management Information System (MIS), Passport Records Imaging System Management (PRISM), and Passport Lookout Tracking System (PLOTS) are created and assigned the appropriate privileges in UMWS. The user then can perform the tasks associated with the privileges.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?
Yes, the information relates to passport issues and management of the passport application process.

(c) Does the system analyze the information stored in it? ☐ Yes  ☒ No
If yes:
(1) What types of methods are used to analyze the information?
(2) Does the analysis result in new information?
(3) Will the new information be placed in the individual’s record? ☐ Yes ☐ No
(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☐ Yes ☐ No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.
   The information is shared internally within the Bureau of Consular Affairs to include Passport agencies and the Passport Services Directorate, and with the Bureau of Diplomatic Security. Information is not directly shared with any external organizations.
   PLOTS with Diplomatic Security.
   PIERS information is indirectly shared with DHS via the Consular Consolidated Database (CCD). Queries are made via the CCD and provided to DHS.
   PDITS shares information with the Department of Homeland Security. The Consular Data Information Transfer System (CDITS) queries PDITS and provides information to the Passport DHS Senior Agency Official for Privacy (SAOP).

(b) What information will be shared?
   Information about passport applicants, status of applications, all records of issued and expired passports, not issued applications, and destroyed/stolen/lost passports.

(c) What is the purpose for sharing the information?
   The information is shared to assist the Department of State in managing and tracking the passport application process.

Sharing of information externally is a means to verify data and to acquire information on any possible issues regarding applicants for adjudication. Information shared with DHS is to validate and authorize admissions and exits of persons in the U.S.

(d) The information to be shared is transmitted or disclosed by what methods?
   All information is shared using Department of State approved Information System Connection Ports, Protocols and Services.

   Internal Information Sharing:

   Internal information is shared by direct secured communications (data-base to database) using transport and message level security interfaces with other Consular systems and U.S. mail.
PLOTS information is shared internally with Diplomatic Security by utilizing the State Department secure internal network. Information is shared by secure transmission of sensitive but unclassified information in accordance with the Department of State policy for handling and transmission of sensitive but unclassified information.

External Information Sharing:

PIERS Information shared externally with DHS is through CCD, utilizing secure transport layer security methods permitted under Department of State policy for handling and transmission of sensitive but unclassified information.

PDITS information shared through CDITS with the DHS, utilizes secure transport layer security methods permitted under Department of State policy for handling and transmission of sensitive but unclassified information.

(e) What safeguards are in place for each internal or external sharing arrangement?

Internal recipients, within the Department of State, must comply with U.S. government requirements for the protection and use of PII. These safeguards include but are not limited to security training and internal Department policy for the handling and transmission of “Sensitive but Unclassified” information. In addition, all Department users are required to attend annual privacy and security awareness training to reinforce safe handling practices. Data shared with other government agencies (DHS) is carefully regulated according to Memorandums of Agreement/ or Understanding (MOA/U) formally signed by Authorizing Officials of the agency.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk: 1) accidental disclosure of information to non-authorized parties, or 2) deliberate disclosure/theft of information regardless of whether the motivation was monetary, personal or other. Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to-know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

The Department of State mitigates these risks by enforcing rules and requirements regarding:
- Frequent, regular security training for all personnel regarding information security, including the safe handling and storage of PII, “Sensitive But Unclassified,” and all higher levels of classification;
• Strict access control based on roles and responsibilities, authorization and need-to-know;
• Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?
The system contains Privacy Act-covered records; therefore, notification and redress are the right of record subjects. Procedures for notification and redress are published in the System of Records Notice (SORN) Passport Records - STATE-26, and in rules published within 22 CFR Part 171.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?
☒ Yes ☐ No

If yes, explain the procedures.
Individuals who wish to obtain their records or have them amended must submit a written request to the U.S. Department of State, Office of Law Enforcement Liaison Division (CA/PPT/S/L/LE) at the address cited in the Passport Records SORN, STATE-26, posted on the Department of State Privacy website.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?
Individuals who wish to have their records amended can find instructions, submission requirements, and the address of the U.S. Department of State, Office of Law Enforcement Liaison Division (CA/PPT/S/L/LE) in the Passport Records SORN, STATE-26, posted on the Department of State’s Privacy website, www.state.gov/privacy.

8. Security Controls

(a) How is the information in the system secured?
The PAMS system is secured within the Department of State intranet where risk factors are mitigated through the use of multiple layers of security controls, including management security, auditing, firewalls, and physical security.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.
As a matter of policy, the Department of State Chief Information Officer and Information System Security Officer require certain fundamental procedures for all systems. Potential
users are screened and assigned privileges based on their roles, responsibilities and the need-to-know. Specific privileges for a given user are only granted after careful consideration of the user role. There are three types of PAMS user roles: System/Web Administrators, Application Administrators and Database Administrators. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on any changes (authorized or not) that occur to data in the PAMS applications are recorded. In accordance with Department of State Security Configuration Guides, auditing is enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on until the time he/she signed off. This multilayered approach to security controls greatly reduces the risk that PII will be misused.

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, PAMS users are required to complete the annual Cyber Security Awareness Training and the privacy training, PA 459 Protecting Personally Identifiable Information. The Department’s standard “Rules of Behavior” regarding the use of any computer system and the data it contains note that users have an obligation to protect PII through appropriate safeguards to ensure security, privacy and integrity. The following list details some, but not all, of the numerous requirements covered under the “Rules of Behavior” related to PII.

Users are prohibited from the following activities:

- Browsing PII records without authorization or for purposes other than those directly connected with their official work-related responsibilities;
• Disclosing PII to others, including other authorized users, unless there is a need to do so in the performance of official duties;
• Removing PII from the workplace, unless it is for an approved work-related purpose;
• Storing PII in shared electronic folders or shared network files;
• Storing PII on any computing device not owned by the government;
• Altering or deleting PII, unless the action is part of their official duties and responsibilities.

Users are also required to take the following actions:
• Protect access to all media on which PII is processed;
• Store hard-copy PII in locked containers or rooms;
• Safeguard any PII (electronic or hard-copy) which is removed from the workplace in the performance of official duties;
• Protect against eavesdropping on telephones or other conversation when PII is discussed.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?
☒ Yes ☐ No

If yes, please explain.

Bureau of Diplomatic Security (DS) guidelines are implemented for operating systems, web servers, and databases to prevent unauthorized disclosure of information and detect changes to information during transmission.

Systems use Transmission Control Protocol/Internet Protocol TCP/IP to assist with its data transport across the network. The TCP/IP protocol suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including hand-shaking, header checks, and re-sending of data if necessary. Additionally, systems employ the use of Hash message authentication codes to sign packets verifying that the information received by the system from the Internet is exactly the same as the information sent. Also, the Systems Integrity Division is responsible for developing policies regarding digital certificates (including web-based Secure Socket Layer (SSL) certificates), and all cryptographic keys.

The Information Integrity Branch provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. IIB’s goal is to ensure that information processed and stored is safe from unauthorized access, disclosure, disruption, or denial of service. The Information Integrity Branch (IIB) is composed of four operational elements:
• Antivirus
- Mainframe Security
- The Public Key Infrastructure (PKI) and Biometrics
- E-Authentication

All systems must comply with all guidelines published by Systems Integrity Division, in addition to all security configuration guides published by Diplomatic Security. Adherence to these guides is verified during the system’s A&A process.

(f) How were the security measures above influenced by the type of information collected?

The Department of State has long been concerned with the protection of individuals’ personal information in accordance with U.S. government policies. Passport information and the PII contained therein constitute the substantive portion of the information contained in PAMS. Accordingly, the Department of State has implemented the rigorous security measures outlined above to ensure that individuals’ PII is appropriately protected.

9. Data Access

(a) Who has access to data in the system?
The following personnel have access to these systems:
- System/Web Administrators, Application Administrators and Database Administrators

(b) How is access to data in the system determined?
An individual’s job function determines what data can be accessed as approved by the supervisor and ISSO.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No
Consular Affairs/Consular Shared Tabled (CA/CST) adheres to a formal, documented audit and accountability policy that addresses purpose, scope, roles, and responsibilities. In addition, there are documented procedures to facilitate the implementation of the policy and the audit and accountability controls.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.
There are three types of PAMS user roles: System/Web Administrators, Application Administrators and Database Administrators. Users will have access based on the roles/job functions.

**The System/Web Administrator** - The System Service and Operations Project Manager complete the CA/CST System Administrator Account Request Form. The Project Manager signs the form authorizing the account to be established and activated, and a current System Administrator creates the account.
**Application Administrators**- The System Administrators and PAMS Application Administrator users are responsible for establishing, activating, modifying, reviewing, disabling, and removing Application Administrator accounts in the PAMS OpenNet database server.

**Database Administrators**- Database Administrator (DBA) access is controlled by the Data Integrated Services (IS) team. PAMS DBAs are authenticated using Windows operating system authentication only. The IS Government Technical Monitor is responsible for reviewing and approving accounts. The current DBA activates/establishes an account when he/she adds the new user to the Windows security group. Access is disabled when no longer required; accounts are reviewed every 60 days to determine when access should no longer be granted.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data?

Defense in Depth (boundary defense is inherited); Separation of Duties

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing. Audit logs are reviewed at the Application, Database, and System level as follows:

**Application level**: PAMS administrators review the application level audit logs as necessary and take the appropriate action if suspicious activity or suspected violations are identified.

**Database level**: The System Security Officer (SSO) reviews the Structured Query Language (SQL) logs for indications of inappropriate or unusual activity on the PAMS database, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.

**System level**: The SSO reviews the Operating System (OS) logs for indications of inappropriate or unusual activity on the PAMS system, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.