PRIVACY IMPACT ASSESSMENT

Passport Lookout Tracking System (PLOTS) PIA

1. Contact Information

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

2. System Information

(a) Name of system: Passport Lookout Tracking System (PLOTS) PIA

(b) Bureau: Consular Affairs

(c) System acronym: CA PLOTS

(d) iMatrix Asset ID Number: # 346

(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 The authorization is valid until rescinded or the expiry date of July 31, 2019.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:

PLOTS is a Department of State web-based application that supports the Bureau of Consular Affairs mission requirements by enabling users to manage and track PLOTS cases. PLOTS is used by Passport services, other Consular Affairs offices, and Diplomatic Security to manage passport lookout cases. A Lookout case is a file documenting the basis for denial or potential denial of a passport application, or for initiation of a civil or criminal investigation. Lookout cases may involve fraud or fraud prevention, false identity, international parental

child abduction or prevention, indebtedness to the federal government, citizenship loss or non-acquisition, as well as other matters.

PLOTS streamlines the Passport Lookout tracking process and shortens the duration of investigations by eliminating the need to physically transfer hard copy files, so that the lookout cases can be efficiently processed by enabling users to:

- Create and modify new cases and Lookout records
- Search, retrieve, and manage existing cases and Lookout records
- Search, add, and delete Lookout records in the Consular Lookout and Support System (CLASS)
- Refer cases electronically to Diplomatic Security (DS)

This is accomplished through interfaces and connections with other State applications as follows: PLOTS connects to and shares information with the User Manager Web Security (UMWS), the Investigation Management System (IMS) and Management Information System (MIS) through a web service and with the Consular Consolidated Database Enterprise Case Assessment Service (CCD-ECAS), Consular Lookout and Support System (CLASS), Passport Records Imaging System Management (PRISM), Passport Information Electronic Records System (PIERS), and the Travel Document Issuance System (TDIS) through an interface with the Front End Processor (FEP) database.

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

- Name
- Birthdate
- Social Security Number or other Identifying Number
- Phone Number(s)
- Business Addresses
- Home Addresses
- Email Addresses of Individuals
- Images or Biometrics Identifiers
- Financial Transactions
- Medical information
- Employment information
- Legal/criminal information
- Driver’s license information/photocopy
- Passport number

(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, 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. Subchapter F (Nationality 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)
- Executive Order 9397, November 22, 1943; Executive Order 13478, November 18, 2008

(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, and Other Overseas 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-13-001-16 Passport Lookout Master

Description: This on line 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?

Passport application information listed in paragraph (4d) and supporting information are retrieved from the Consular Affairs TDIS, CLASS, CCD-ECAS and PRISM systems to create and manage Lookout cases. Information in PLOTS is not collected directly from the applicants. PLOTS passport information about applicants is obtained from the CA Systems listed above.

(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, other CA systems which interface with law enforcement systems and systems at the Social Security Administration, Internal Revenue Service and the Department of Homeland Security.

Quality control measures based on layered approvals ensure that Lookouts and other information (e.g., diary entries) entered in the case file by consular officers and passport specialists are accurate and relevant to the record subject.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Information is updated in the source system when a new application is filed or updated. The applicant prepares the application for the requested service either in paper form or online depending on the requirement. Updated information is retrieved from the source systems addressed in paragraph 4(c) in managing Lookout cases.

(g) Does the system use information from commercial sources? Is the information publicly available?
No, the system does not acquire information from commercial sources nor is the information publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?

This is not applicable because no data is entered into PLOTS directly by individuals. The notice is provided to applicants upon submission of applications for passport services. Individuals grant consent via the passport application process.

(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?

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

No data is entered into PLOTS by passport applicants. All data transmitted by the PLOTS system is from other CA systems listed in paragraph 4(c) or diary information entered by passport specialists at passport agencies/centers and at overseas posts. Individuals grant consent via the passport application process at the point of entry of information.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

PLOTS does not collect data as information in the PLOTS system is retrieved from other CA systems listed in paragraph 4(c).

The PII in PLOTS is the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. The collection of PII is limited to only what is required for the systems to perform the functions for which it is intended to support the management of passports.

5. Use of information

(a) What is/are the intended use(s) for the information?

PLOTS information is used by the Bureau of Consular Affairs Directorate of Passport Services, other Consular Affairs offices, and the Bureau of Diplomatic Security to manage the processing of passports. Information contained in PLOTS allows these users to manage and track a passport lookout case. Lookouts data alerts passport specialists of possible fraud or other possible irregularities such as a person having the same or similar name and date of birth as that of the applicant. PLOTS information assists in determining whether to deny a passport application or initiate a criminal investigation, and may relate to fraud and fraud prevention, a child in the Children's Passport Alert Program or issues related to verifying the applicant's citizenship or identity.

(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 assists in the operations 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.

Consular Affairs TDIS, CLASS, CCD-ECAS and PRISM systems share information in paragraph 3(d) with PLOTS to create and manage Lookout cases. Other information acquired from these systems may also involve fraud or fraud prevention, false identity, international parental child abduction or prevention, indebtedness to the federal government, citizenship loss or non-acquisition, as well as other matters.

UMWS is the application used to manage user accounts, passwords, and privileges for many passport applications.

The Management Information System (MIS) acquires information from PLOTS to generate passport management reports and documents.

Lookouts are created by passport specialists at passport agencies/centers and at overseas posts in PLOTS which are then entered manually into the Consular Lookout and Support System (CLASS).

(b) What information will be shared?
PII in paragraph 3.c. will be shared in addition to information about passport applicants, status of applications, all records of issued and expired passports, not issued applications, irregularities, 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 developing and managing Lookout cases and the passport application process. Sharing of information is a means to verify data and to acquire information on any possible issues regarding applicants for adjudication.

(d) The information to be shared is transmitted or disclosed by what methods?
All information is shared using Department of State approved secure Information System Connection Ports, Protocols and Services. All of the CA systems reside on the Department's secure intranet network, OpenNet.

Internal information is shared through interfaces and connections with other CA systems using transport and message level security interfaces with other Consular systems listed in paragraph 4(c).

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

Information is shared internally to manage Lookout cases and the passport review processes. Supervisors along with information system security officers determine the access level depending on job function and level of clearance. Recipients within the Department of State must comply with U.S. government requirements for the protection and use of PII.

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Access to electronic files is protected by inherited security controls from the DoS domain infrastructure. All accounts are under the supervision of system managers. Audit trails track and monitor usage and access.

In addition, all Department users are required to attend privacy and security awareness training to reinforce safe handling practices. Defense in depth is deployed as well as role based access based on least privilege.

(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, and 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?
No information is collected from individuals into PLOTS. PLOTS information is obtained from other CA systems outlined in paragraph 4(c). The individual would need to follow processes outlined by the source system used to request services to access their information.

Individuals can also follow procedures outlined in the Passport Records SORN, STATE 26 posted on the Department of State's Privacy website.

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

If yes, explain the procedures.

If no, explain why not.
PLOTS does not collect information from applicants requesting services. Individuals must follow processes of the source systems used to apply for the specific service to request correction of information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can also follow procedures outlined in the Passport Records SORN, STATE 26 posted on the Department of State's Privacy website.

(c) By what means are individuals notified of the procedures to correct their information?
This is not applicable, as PLOTS does not collect information from individuals.

However, notice to correct personal information is provided at the source site where applicants apply for specific passport services.

Individuals who wish to have their records amended can also find instructions, submission requirements, and the address of the U.S. Department of State, Passport Services, Office of Legal Affairs, 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?

PLOTS is secured within the Department of State intranet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

CA Systems are configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and are tracked until compliant or acceptably mitigated.

(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.

To access the system, persons must be authorized users of the Department of State's unclassified network which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must sign the user access agreement/rules of behavior before being given a user account. Authorized users have been issued a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal system access and is required for logon.

Access to the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports that are to be restricted. Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(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 network (OpenNet) and respective

applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also 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, mandatory security (PS800 Cyber Security Awareness) and privacy (PA459 Protecting Personally Identifiable Information) training is required for all authorized users. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources.
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 Assessment and Authorization process.

PLOTS use Transmission Control Protocol/Internet Protocol TCP/IP to assist with its data transport across the network. Data in transit is encrypted. The TCP/IP 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.

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

The information collected contains PII of U.S. Citizens and Legal Permanent Residents (LPR). Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

The following personnel have access to these systems:
Department of State employees and contractors working domestically and overseas in connection with processing passports; System 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 the Information Systems Security Officer. Access is role based and the user is granted only the role(s) required to perform officially assigned duties.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented?

☒Yes ☐No

Consular Affairs/Consular Systems and Technology (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 PLOTS user roles: Department of State employees and contractors, System Administrators and Database Administrators. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

PLOTS OpenNet Users- Access to PLOTS is restricted to cleared Department of State direct hire and contractor employees. DoS employees and contractors receive their access by requesting access from the CA organization in compliance with 12 FAM policies. Each user must submit an OpenNet Account Request Form indicating the system he/she needs access to in order to do his/her job. The account request is reviewed by the user's supervisor and must be approved by the system manager before the request can be granted.

The System Administrator- The System Service and Operations Project Manager completes the CA/CST System Administrator Account Request Form. The Project Manager reviews the role and approves the form authorizing the account to be established and activated, and a current System Administrator creates the account.

Database Administrators- Database Administrator (DBA) access is controlled by the Data Integrated Services (IS) team. 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 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? PLOTS information is protected by multiple layers of security controls including:

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented; access is role based as required by policy.

- PLOTS System & Database Administrators and internal users have access via OpenNet from the Department of State configured workstations. Users must dual factor authenticate utilizing Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) to access data. Users are uniquely identified and authenticated before accessing PII and while logged in can be traced to the person who performed the activity.

- Least Privileges are restrictive rights/privileges of or access by users for the

performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.

In addition to the restrictions mentioned above in section 9(d), all accounts are subject to automatic auditing.