Online Passport Lost & Stolen System (OPLSS)

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 31, 2008

(b) Name of system: Online Passport Lost & Stolen System

(c) System acronym: OPLSS

(d) IT Asset Baseline (ITAB) number: 2751

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

The Online Passport Lost & Stolen System permits citizens to report a lost or stolen passport using the Internet and a standard browser. The concept of OPLSS will decrease the burden of work for employees at the National Processing Information Center (NPIC) and will effectively permit U.S. citizens to report a lost or stolen passport 24 hours a day, 7 days a week and 365 days a year (24/7/365) via the internet.

(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 28, 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?

Name, date of birth (DOB), social security number (SSN), address, telephone number, and e-mail address. The source of the information provided to OPLSS is U.S. citizens reporting lost or stolen passports.

b. How is the information collected?

Information is collected via the internet and a standard web browser to provide U.S. citizens the ability to report lost or stolen passports. The information is collected directly from U.S. citizens inputting their personally identifiable information into OPLSS via a web interface.

Specifically, public internet users will navigate to the OPLSS Public Web Page within the DoS Public Demilitarize Zone (DMZ) and fill out the DS-0064, “Statement Regarding a Lost or Stolen Passport.” The OPLSS OpenNet Database server is scheduled to pull all data from the DMZ Database every ten minutes. All records will then be deleted from the DMZ Database.

c. Why is the information collected and maintained?

Information is collected to provide U.S. citizens the ability to report lost or stolen passports via the internet and a standard web browser.

d. How will the information be checked for accuracy?

It is the responsibility of the U.S. citizen reporting a lost or stolen passport that their information is accurate and complete. However, once data is input into OPLSS, information reported from U.S. citizens will be verified for accuracy by comparing the information stored in the Passport Information Electronic Records System (PIERS) owned and operated by the Bureau of Consular Affairs (CA).

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

- 8 U.S.C. 1401–1503 (2007) (Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)
- 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)
- 22 U.S.C. 211a–218, 2651a, 2705
- 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. 1185 (Travel Control of Citizens)

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 (eg, firewalls, intrusion detection systems, antivirus software), and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

The information is used by CA's administrators and analysts to participate in the coordination efforts to effectively capture data/information associated with a Lost or Stolen Passport; to maintain accurate and timely information; thus, establishing uniform procedures for the reporting, recording, processing, and possible referral to Diplomatic Security (DS), as appropriate, for investigation of Lost or Stolen Passport.

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

Analysis of the information is limited to non-subject-based statistical information, such as the number of passports, lost or stolen on an aggregate cycle (i.e., Monthly, Quarterly, Yearly, etc.) Furthermore, no new information is derived.

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

The system does not use any commercial information, publicly available information, or information from other Federal agency databases. All of the information in the system is derived from passport applications and vital records collected and maintained by Consular Affairs.

d. Is the system a contractor used and owned system?

The Department of State (DoS) owns the system and contractors are the primary designers and developers of the OPLSS. All contractors have abided to regulatory guidelines and have signed and follow CA's Rules of Behavior.

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.

OPLSS 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 OPLSS 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 OPLSS 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 retention period of information is consistent with established Department of State Policies and Guidelines as documented in the DoS Disposition Schedule, Chapter 13, Passport Records.

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

None. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in Chapter 13 Passport Records. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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?

The information in OPLSS is shared with FEP, PIERS and CLASP which are owned and operated by CA. CA/CST is responsible for protecting the privacy rights of the public and employees affected by the interfaces.

Access to OPLSS servers is restricted to approved contractors, managers and system administrators based on access controls and the permissions of the role the person is placed in. Direct system access is not provided to non-Department entities. Department employees will be able to search OPLSS database and retrieve records from an internal website using the individual's name, and DOB/SSN. Access to the internal web site is restricted to authorized users.

Additionally, the information will be referred to Diplomatic Security (DS) within the Department of State, as appropriate, for investigation of the following:

(1) Cases of lost, stolen, and found valid U.S. passports;

(2) Cases of altered, damaged or mutilated U.S. passports; and

(3) The valid search of the Passport Information and Electronic Records (PIERS) and Consular Lost and Stolen Passports (CLASP) databases to verify whether an applicant has previously obtained a valid or expired, regular passport and/or reported said passport lost or stolen.

Moreover, only the relevant information that is needed to conduct the investigation is passed on to DS.

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

Consular Affairs users will navigate to the Internal Administration Web Page within the Department's OpenNet and process Form DS-0064, "Statement Regarding a Lost or Stolen Passport" for any records received from the public web site. All records of Form DS-64, "Statement Regarding a lost or Stolen Passport," are stored in the OPLSS Database within OpenNet. Passport information in the form of XML data packets are pulled from the PIERS systems via FEP into the OPLSS Web Server. Each record has a unique identifier and is traceable.

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?

OPLSS does not interface with external entities. Persons or government agencies external to the Department of State's OpenNet are not able to access information within OPLSS.

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 OPLSS. 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

☐ does NOT contain information covered by the Privacy Act.

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

Notice of the purpose, use and authority for collection of information submitted are described in the System of Records Notices titled STATE-26, Passport Systems.

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

Before completing an online passport application form (that is, the DS-11 Form), the individual is presented with a Privacy Act statement. Acknowledgement of the Privacy Act notice signifies the individual's consent to the use of his or her information. Notice of the purpose, use and authority for collection of information submitted are also described in the System of Records Notice titled STATE-26, Passport Systems.

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. The utility of the information in the system about a particular individual will not extend over the allotted time in the Department of State's Disposition of Schedule, as defined in

Chapter 13 Passport Records. Moreover, there is negligible privacy risk as a result of degradation of its information quality over an extended period of time.

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?

OPLSS 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 OPLSS is limited to authorized Department of State staff having a need for the system in the performance of their official duties. All authorized government users maintain a security clearance level at least commensurate with public trust positions. To access the system, the individual must first be an authorized user of the Department's unclassified computer network.

The information 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 seen and the degree to which data may be modified. A system use notification ("warning banner") is displayed before log-on is permitted, and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

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

CA Security and Diplomatic Security uses an array of configuration auditing and vulnerability scanning tools and techniques to periodically monitor the OpenNet-connected systems that host CA's major and minor applications, including the OPLSS components, for changes to the DoS mandated security controls.

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 involves privacy risk?

OPLSS operates under standard, commercially-available software products residing on a government-operated computing platforms not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are employed in OPLSS.

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 OPLSS.

12. Security

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

The Department of State operates OPLSS 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, OPLSS was certified and accredited on August 1, 2007. This authority to operate is valid until August 2010.