DEPARTMENT OF STATE

PRIVACY IMPACT ASSESSMENT

Online Passport Lost and Stolen System (OPLSS)
February 28, 2008

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (A/ISS/IPS/PRV)
Email: PIA@state.gov

PRIVACY IMPACT ASSESSMENT

A. CONTACT INFORMATION:

1) Who is the Agency Privacy Coordinator who is conducting this assessment? (Name, organization, and contact information).

Ms. Margaret Grafeld, Director
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION:

1) Does this system collect, maintain or disseminate personally identifiable information about individual members of the public?

YES _X__ NO___

****"Personally identifiable information from/about individual members of the public" means personally identifiable information from/about "any person not acting in his/her official capacity as a federal government employee/contractor". If answer is yes, please complete the survey in its entirety.**

If answer is no, please complete the certification page and submit the PIA to both of the following e-mail address: pia@state.gov

2) Does a Privacy Act system of records already exist?

YES _X__ NO___

If yes, please provide the following:
System Name __Passport Records__ Number __State-26__

If no, a Privacy system of records description will need to be created for this data.

3) What is the purpose of the system/application?

The Online Passport Lost & Stolen System (OPLSS) permits U.S. citizens to report a lost or stolen passport using the Internet and a standard browser. Currently, U.S. citizens can only report lost or stolen passports via telephone to

the National Passport Information Center (NPIC) during the hours of 6 a.m. to midnight, ET, Monday-Friday, excluding Federal holidays.

The concept of OPLSS will decrease the burden of work for employees at the 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.

4) What legal authority authorizes the purchase or development of this system/application?

Passport Services has requested this application to comply with the E-Gov Act of 2002 and to provide U.S. citizens with a view into services the U.S. Government provides them.

Titles 8 & 22 of US Code 22 U.S.C 1101
Executive Order 11295, (August 5, 1996) Part 1, Title 22 Code of Federal Regulations (CFR)

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

U.S. citizens with a previously issued domestic passport that wish to report it loss or theft, or the loss or theft of passport for a person whom the reporting citizen can act as the legal guardian representative.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

U.S. citizens reporting lost or stolen passports.

b. What type of information is collected from the source of the information?

Name, date of birth (DOB), social security number (SSN), address, telephone number, and e-mail address.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

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 CA.

b. How will data be checked for completeness?

The online Form DS-0064 form has built in validation routines to ensure all mandatory fields are complete. The Form DS-0064 has been in existence since 2006 and has an expiration date of 3-31-2009.

c. Is the data current?

Yes. Public users will navigate to the OPLSS Public Web Page within the DoS Public DMZ and fill out the Form DS-0064 "Statement Regarding a Lost or Stolen Passport." The information is temporarily stored in the Data DMZ Database. The OPLSS OpenNet Database server is scheduled to PULL all data from the DMZ Database every 10 minutes. All records will then be deleted from the DMZ Database. The Bureau of Consular Affairs users will navigate to the internal Administration Web Page within the DoS OpenNet and process the 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 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.

D. INTENDED USE OF THE DATA:

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

The use of the data will be both relevant and necessary to the purpose for which the system is being designed.

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

There will be no new data or previously unavailable personal data created through derived data or aggregation of data collected.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

The system will not make determinations about DoS employees or the public as no new data is created.

4) **Will the new data be placed in the individual's record?**

No new data will be placed in the individual's record.

5) **How will the new data be verified for relevance and accuracy?**

No new data is created; therefore, it does not need to be verified for relevance and accuracy.

6) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

DoS employees will be able to search OPLSS database and retrieve records from an internal website using the individual's name, DOB, and/or SSN. Access to the internal web site is restricted to authorized users. Internet users will navigate to the OPLSS Public Web Page within the Department's Public DMA and fill out Form 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. This will prevent the internet users from going back and looking at their information for case updates.

7) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

No reports are created.

E. MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:

1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

The OPLSS system is deployed only to a single set of servers in the DMZ and OpenNet. The OPLSS OpenNet Database server will pull all data from the DMZ Database every 10 minutes.

2) **What are the retention periods of data in this system?**

The retention period of OPLSS data is 120 days. Data older than this period will be purged from the system.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

An update package, run daily, deletes from the table all information older than the 120 days retention period. These procedures are documented in the OPLSS SSP dated March 2008.

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

OPLSS is not using any technologies not previously employed at the Department of State.

5) **How does the use of this technology affect public/employee privacy and how does it restrict access to the system?**

N/A.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

The system does not provide monitoring.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

No – the system is not being modified.

8) **Are there forms associated with the system? YES_X__ NO___**
If yes, do the forms include Privacy Act statements that include required information (e.g., - legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided.

Yes, the form does include a Privacy Act statement that includes required information and the effects on the individual if the data is not provided.

F. ACCESS TO DATA:

1) **Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, other)**

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 individuals name, and DOB/SSN. Access to the internal web site is restricted to authorized users.

Public Internet users will navigate to the OPLSS Public Web Page within the DoS Public 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.

2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?

The Public Internet Users of OPLSS will access the system from remote, non-Department of State personal computers, over which neither the Department nor the Bureau of Consular Affairs has control (i.e. user's PC hardware/software, printer, Internet connection). However, in order to access OPLSS, the end-user's browser must be able to support 128-bit encryption that will be forced by the use of Secure Sockets Layer (SSL). The OPLSS web server will be configured to only allow SSL connection through the use of a CA-purchased VeriSign Global Secure Server ID (SSL certificate).

Communications security (COMSEC) elements for the OPLSS systems secure communication are based on Public Key Infrastructure (PKI) technologies. The use of the PKI-enabled digital server ID provides the security qualities of accountability, authentication, integrity, and non-repudiation.

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.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Users will be allowed to input their own information and will not have access to other information. Access is restricted to a single session. Users will not

be given logon access or be allowed to return at a later time to finish a transaction started previously.

4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access?**
(Please list processes and training materials)

All user connections to the public web server are encrypted using a 128-bit SSL server certificate. The web server utilizes Public Key Infrastructure (PKI) and requires a public key that matches the private key. Once the SSL public and private handshake is completed, the connection is encrypted and all data transmitted from either end is encrypted. Individuals accessing the OPLSS web site will not be permitted to add, change or delete data contained in OPLSS. The OPLSS OpenNet Database server is scheduled to pull all data from the DMZ Database every 10 minutes. All records will then be deleted from the DMZ Database therefore no data is stored.

5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

Yes. 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.

6) **Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

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 to the public and employees affected by the interfaces.

7) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?**

The information in OPLSS is <u>not</u> shared with other agencies.

8) **Who is responsible for assuring proper use of the shared data?**

CA/CST is responsible for shared data within the Department.