

Consular Lookout and Support System (CLASS)

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 2, 2008
- (b) Name of system: Consular Lookout and Support System
- (c) System acronym: CLASS
- (d) IT Asset Baseline (ITAB) number: 558
- (e) System description (Briefly describe scope, purpose, and major functions):
The Consular Lookout and Support System (CLASS) is used by Department of State (DoS) passport agencies, posts, and border inspection agencies to perform name checks on visa and passport applicants to identify individuals who may be ineligible for issuance or require other special action. The Passport Lookouts and Visa Lookouts are separated to ensure proper handling and disclosure of information. The Passport Lookouts can be either U.S. persons or foreign persons, e.g. someone making a false claim to U.S. citizenship. The Visa Lookouts are primarily foreign persons with some infrequent secondary data that may refer to a U.S. person.
- (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):
- (h) Date of previous PIA (if applicable): October 30, 2005

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.

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

With respect to U.S. visa applicant information maintained in CLASS, such information is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

Because visa applicants themselves are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the Privacy Act. However, the visa portion of CLASS records may include PII about persons associated with the visa applicant who are U.S. citizens or legal permanent residents.

With respect to U.S. passport application information maintained in CLASS, elements of PII collected and maintained include but are not limited to: passport applicant name; date of birth; country or place of birth; gender; aliases; passport number; alien registration number (aliens only); national ID (aliens only); SSN (U.S. citizens only); and physical description.

Information collected and maintained by CLASS is obtained directly from passport and visa applicants and enhanced with information collected from DoS lookout lists and external agencies. The initial applicant information is collected by other DoS systems (listed below) and transferred to CLASS for namecheck and lookout search purposes.

b. How is the information collected?

Information in CLASS is not obtained directly from the individuals. If an applicant is refused a visa or passport, the information is forwarded from the Visa or Passport Office, originally scanned from the applicant's current passport and/or collected from the visa application form. Department of State system sources include:

- Non-Immigrant Visa (NIV);
- Immigrant Visa (IV);
- Visa Opinion Information Service (VOIS);
- Waiver Review System (WRS);
- Consular Consolidated Database (CCD);
- American Citizen Services (ACS);
- Independent Name Check (INK);
- Travel Document Issuance System (TDIS); and
- Passport Lookout Tracking System (PLOTS).

Information in CLASS may also be obtained independent of an application. Information involved in law enforcement, national security, and U.S. Border security is forwarded from the following U.S. Government agencies:

- International Criminal Police Organization (Interpol);
- Health and Human Services (HHS);
- Department of Homeland Security (DHS);
- U.S. Marshall Service (USMS);
- Federal Bureau of Investigation (FBI);
- Terrorist Screening Center (TSC);
- Drug Enforcement Administration (DEA); and
- Treasury Enforcement and Communication System (TECS).

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

c. Why is the information collected and maintained?

Information is collected for passport agencies, consulates, and border inspection agencies to perform name checks of visa and passport applicants in support of issuance processing and document verification. CLASS performs name checks on U.S. passport applicants and on aliens seeking visas in order to identify individuals who are ineligible for visa or passport documentation or who require special action.

d. How will the information be checked for accuracy?

Accuracy is the responsibility of the passport or visa applicant and the agency that originally collected the additional lookout data. Any errors detected by the CLASS team or during Visa or Passport issuance are called to the attention of the owning agency.

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

8 U.S.C. 1101-1503 (Immigration and Nationality Act of 1952, as amended)

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

The CLASS system collects the minimum amount of information required to satisfy the statutory purposes of the system and the mission of the bureau. The information collected by CLASS is the minimum required to perform name checks on visa and passport applicants in support of the issuance process.

To protect the data there are numerous management, operational, internal, and technical security controls implemented 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 security, encryption, role-based access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), annual training and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

CLASS data is used to support the visa and passport issuance process. CLASS performs name checks on U.S. passport applicants and on aliens seeking visas in order to identify individuals who are ineligible for visa and passport issuance or who require special action.

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

The data is analyzed by adjudicators during the visa/passport adjudication process. CLASS may derive spelling variations of names involved in the namecheck process to

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

improve recall in the namecheck search algorithms and may be modified when the spelling variation mappings are changed, or the algorithm software is modified.

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

CLASS does not use commercial/publicly available information; rather, it uses information regarding individuals collected from government agencies involved in law enforcement, national security, and U.S. border protection. See sections 3b and 3c above for an explanation of how this data is used.

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

The system is owned by DoS, but is operated and maintained by contractors who are required to maintain at least a secret clearance.

All contract personnel must pass a National Agency Check and Diplomatic Security processing. The contractor facilities where CLASS is maintained are under 24/7 security watch, 365 days a year by the DoS personnel. In addition, access to the server rooms is protected by an electronic entrance combination lock as prescribed by internal DoS policy.

Development staff is also primarily contract staff who are required to pass a minimum of a National Agency Check. Developers have access only to the development region of CLASS.

Second Level Support (2LS) provides operations support of the CLASS production, data quality, and ePilot environments. Its primary responsibility is monitoring the production environment to ensure 24/7 availability of name check and refusal update submission to the user community and to ensure that replication updates between the redundant CLASS sites are current to acceptable standards. All contractors have an approved Privacy Act clause in their contracts and must pass annual security/privacy training.

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.

All contractors must pass a National Agency Check and DOS Diplomatic Security processing and annual security/privacy training (see answer to 4.d above).

Information from other government agencies is transmitted to CLASS dependent upon approved memorandums of understanding (MOUs) that specify strict qualifications for transmission, length of use, and data retirement criteria

All authorized users must pass annual computer security and privacy training. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses. Contractor-owned facilities are annually inspected by DOS Diplomatic Security. Furthermore, system audit trails are automatically generated and regularly analyzed and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of the particular functions a particular user performed--or attempted to perform.)

5. Retention

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

a. How long is information retained?

Retention of these records varies depending upon the specific kind of visa refusal code or passport reason code. The retention period can range from one year for minor issues to 100 years for more serious issues such as suspected terrorism or criminal activity.

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

Files of closed cases are disposed of in accordance with published DoS record schedules as approved by the National Archives and Records Administration (NARA).

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

CLASS information is shared with DoS consular officers who may be handling a legal, technical or procedural question resulting from an application for a U.S. visa or passport.

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

Internally, information is transmitted in XML format to CXI through various existing client applications that are routed through the Front End Processor (FEP) or Telecommunications Manager (TCM) systems, or through the CLASS interface known as WebCLASS (available to a limited number of DoS authorized users) via OpenNet.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

Data transmitted to and from CLASS is protected by robust encryption mechanisms inherent within OpenNet that encrypt the data from domestic and overseas posts to the database. Additionally, direct access to CLASS is limited to authorized users only. Access to CLASS is dependent on completion of a background investigation and an appropriate job need.

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?

CLASS information is shared with the following agencies:

International Police Organization Interpol – In accordance with Interpol mandate to serve as the clearinghouse for the international database of Stolen and Lost Travel Documents (SLTD), CLASS sends Interpol updates three times daily from the U.S. lost and stolen passports database (CLASP).

Terrorist Screening Center (TSC) - CLASS runs daily queries based on visa refusals against the visa Issuance databases in order to determine if a subject of derogatory information was issued a visa before the hit was entered for sharing with TSC.

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

The Treasury Enforcement and Communication System (TECS) – TECS is used extensively by the law enforcement community and at ports of entry to identify individuals and businesses suspected of or involved in violation of federal law. CLASS updates the system in near-real-time with visa refusals and lookouts, foreign lost and stolen passports, and U.S. lost and stolen passports.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Information sent from CLASS to other government agencies is transmitted based upon approved memorandums of understanding (MOU) and interface control documents (ICD) that specify strict qualifications for transmission, length of use, and retirement criteria.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The uses of the information by external agencies are in accordance with statutory authorities and purposes. Information from other government agencies is sent to CLASS based upon approved memorandums of understanding (MOUs) that specify strict qualifications for transmission, length of use, and retirement criteria.

8. Notice

The system:

constitutes a system of records 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):

- Visa Records, STATE-39
- Passport Records, STATE-26

does not constitute a system of records covered by the Privacy Act.

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

This system does not collect personal information directly from any individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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

This system does not collect personal information directly from any individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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?

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

This system does not collect personal information directly from any individuals; therefore, opportunity and/or right to decline options do not apply to this system.

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 notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's purpose 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?

Data within CLASS is amended by authorized users at the agencies and posts. There are no procedures for individuals to gain access to their information and amend it directly in CLASS. However, they may file a complaint with the Department of Homeland Security's Travel Redress Inquiry Program (DHS TRIP). It is a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during their travel screening at transportation hubs--like airports and train stations--or crossing U.S. borders.

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 purposes and uses and its applicable legal requirements.

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?

Access to CLASS is restricted to authorized users with a "need to know" based upon their job need (such as adjudicating visa or passport applications,). CLASS administrators also have access for the purpose of maintenance and production support. All activities are logged and monitored.

b. What privacy orientation or training for the system is provided authorized users?

All users are required to pass annual computer security awareness training/privacy training prior to being permitted access to the system and they must complete annual refresher training in order to retain access.

Privacy Impact Assessment: Consular Lookout and Support System (CLASS)

- 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.**

Access control lists, defining 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 routinely reviewed to deter and detect unauthorized uses. (An audit trail provides a record of the particular functions a particular user performed--or attempted to perform.)

11. Technologies

- a. What technologies are used in the system that involves privacy risk?**

None of the technologies employed by CLASS pose any inherent privacy risks.

- b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.**

Authorized users can access the system depending on their job function. Mandatory technical, security and privacy training inform authorized users of their responsibilities in handling personal information appropriately.

12. Security

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

CLASS is currently operating under full ATO due to expire March 31, 2009. Due to its upcoming expiration, CLASS has entered the Certification phase of the upcoming C&A.