1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: March 16, 2012

(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 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.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): N/A

(h) Date of previous PIA (if applicable): December 2, 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?

The Consular Lookout and Support System (CLASS) is used by Department of State 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.

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 the visa applicants themselves are not U.S. persons (that is, U.S. citizens or an alien lawfully admitted for permanent residence) at the time of application, they are not covered by the provisions of the E-Government Act of 2002, OMB 03-22, and Privacy Act of 1974, as amended. 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 and of visa applicants who have naturalized or become lawful permanent residents, and who are covered by the E-Government Act and Privacy Act.

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 assigned by the Department and collected from Department lookout lists and external agencies. The initial applicant information is collected by other Department systems (listed below) and transferred to CLASS for namecheck and lookout search purposes.

b. How is the information collected?

Information maintained in CLASS is collected, in part, directly from passport and visa applicants on paper or online passport and visa application forms which are received and processed at domestic passport agencies and U.S. embassies and consulates overseas. Information can be collected from the following Department passport and visa application forms:

- Form DS-156: U.S. Department of State Nonimmigrant Visa Application (OMB 1405-0018)
- Form DS-160: U.S. Department of State Online Nonimmigrant Visa Application (OMB 1405-0182)
- Form DS-1648: U.S. Department of State Online Application for A, G, or NATO Visa (OMB 1405-0100)
- Form DS-260: U.S. Department of State Online Immigrant Visa and Alien Registration Application (OMB 1405-0015)
- Form DS-261: U.S. Department of State Choice of Address and Agent (OMB 1405-0126)
- Form DS-5501: Electronic Diversity Visa (eDV) Application (OMB 1405-0153)
- Form DS-11: Application for a U.S. Passport (OMB 1405-0004)
- Form DS-82: U.S. Passport Renewal Application for Eligible Individuals (OMB 1405-0020)
- Form DS-4085: Application for Additional Visa Pages (OMB 1405-0159)
- Form DS-5504: Application for a U.S. Passport - Name Change, Data Correction, and Limited Passport Replacement (OMB 1405-0160)

- Form DS-64: Statement Regarding Lost or Stolen Passport (OMB 1405-0014)

Data from these forms are entered into other Department systems (listed below) and transferred to CLASS for name check and lookout search purposes. 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 Overseas (IVO)
- 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)
- 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)
- United States Marshall Service (USMS)
- Federal Bureau of Investigation (FBI)
- Terrorist Screening Center (TSC)
- Drug Enforcement Administration (DEA)
- Department of Defense (DoD)
- Treasury Enforcement and Communication System (TECS)

c. Why is the information collected and maintained?

Information is collected by passport agencies, U.S. embassies and 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. The elements of PII necessary for name checking functionality are:

- 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).

These groups use various front-end systems that connect to CLASS via the Telecommunications Manager (TCM), Front End Processor (FEP), Enterprise Service Bus (ESB) and Consular Consolidated Database (CCD) systems to perform a name check on every visa and passport applicant. There is no direct access to the CLASS databases that contain the visa and passport records for these users.

There is only one Graphical User Interface (GUI) to CLASS. This interface is called WebCLASS and is implemented as a series of web pages with a user interface that is only available from the Department network. The overall process mimics the behavior of conventional web sites that allow the user to interface with the centralized database. WebCLASS hosts a series of web pages that offer a full range of name check capabilities. Only persons who have been approved by management within the VO/I and PPT/TO offices have access to WebCLASS.

d. How will the information be checked for accuracy?

The elements of PII used to perform a passport or visa name check query are:

- 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).

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. The CLASS Operations team ensures replication updates between the redundant CLASS sites is current to acceptable standards. Included in the submission of updates to/from CLASS are external agency feeds. External agency feeds requiring manual processing are administered by Operations and in some cases involve locating and correcting data format discrepancies. The Operations Support team troubleshoots issues directly or coordinates third level support as needed.

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

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- INA, 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 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)
- INA, 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)
- 22 U.S.C 2651(a) (Organization of Department of State)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

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. However, with the collection of passport data, CLASS has high data element sensitivity and high data subject distinguishability.

Due to the strict security controls required by all Department of State systems before system operation commences, privacy risks are generally limited to three categories. The most common ways in which PII can become exposed to unauthorized users and potentially vulnerable to identity theft:

- **Device theft or loss** Lost or stolen laptops and other devices such as removable drives may contain PII.

- **Portable Devices** PII is at the fingertips of every staff member who has email, database and Web access at work. The growing use of removable media such as USB drives, CDs/DVDs and portable Mp3 players creates risk by making PII easily transportable on devices that aren't always properly secured.

- **Insider threat** Disgruntled employees seeking revenge or inadvertent human error to send PII over the internet.

The consequences to organizations or individuals whose PII has been exposed to unauthorized users may include the following:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation
- Law enforcement investigations could be compromised

- Delay in processing passport and visa applications or lookouts
- Approving applicants who are not eligible
- Denying applicants who are eligible or imposing unnecessary limitations

To protect the data there are numerous management, operational, internal, and technical security controls implemented in accordance with the Federal Information Security Management Act (FISMA) of 2002 and the information assurance standards published by the National Institute of Standards and Technology (NIST). 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.

The information in CLASS is used to process visa or passport name check queries from WebCLASS or front end client applications. The information in CLASS is also used to run U.S. Consular Lost and Stolen Passport (CLASP) reports, and Lost and Stolen Foreign Passport (LSP) reports from WebCLASS.

The minimum PII required to process a visa name check query are the following: Surname, Given Name, Date of Birth (DOB), Gender, and Country of Birth (COB).

The following information types are not required but can be used in combination with the above PII to process a visa name check query: Country of Citizenship (COC), Passport Number, Passport Book, Other Names (i.e., aliases).

The minimum PII required to process a passport name check query are the following: Surname, Given Name, Date of Birth (DOB), Gender, and Place of Birth Country.

The following information types are not required but can be used in combination with the above PII to process a passport name check query: SSN, Place of Birth State, and Other Names (i.e., aliases).

The minimum PII required to run a CLASP report are the following: SSN and/or Passport Number and/or Surname, Given Name, DOB, Place of Birth Country, and Gender.

There is no PII required to run an LSP report. Only Issuing country and book type information are required for this type of search.

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

Lookouts can be entered in and removed from CLASS several ways. The CLASS component referred to as the CLASS External Interface (CXI) handles visa and passport lookout updates.

When Department-owned visa and passport client systems began having cases that resulted in the generation of passport or visa updates, CXI web services were implemented to facilitate the submittal of such transactions. These services are Passport Lookout Processing Web Service and Visa Lookout Processing Web Service. The transactions originating from the client applications are sent via the Department Front End Processor (FEP) or Telecommunications Manager (TCM). The FEP/TCM sends XML-formatted transactions to the appropriate CXI Web Service. The web service parses the XML and updates CLASS database tables with the lookout data.

Lookout data is also fed to the CLASS database by the Consular Consolidated Database (CCD). CCD populates the CLASS Name check Issuance database with Immigrant Visa and Non Immigrant refusal data from the CCD. This is done via an Oracle database cursor. The cursor will translate the columns from the CCD database to those in the CXI Issuance database kernel tables.

WebCLASS also contains menus to enter and remove lookouts from CLASS. The Visa Lookout Menu within WebCLASS has a button to bring up the Visa Add page, ready for input. WebCLASS users, at a minimum, must be able to provide the following PII to add a visa lookout record to CLASS: Surname, Given Name, Country of Birth (COB), Date of Birth (DOB), Refusal Site, Refusal Code, and Refusal Date. Input validation rules built into the CLASS application logic detect if any errors are in the data. Errors must be corrected before a successful lookout is created.

Clicking the Delete link on a Name check display or Lookout list causes the Visa Delete page to display in a new window, filled by data from the selected record. The WebCLASS user must review the data that is in the record they wish to delete, and click the “Yes” button. Clicking “No” returns the user to the previous display.

Similar to the Visa Lookout, the Passport Lookout Menu has a button to bring up the Passport Add page, ready for input. WebCLASS users, at a minimum, must be able to provide the following PII to add a passport lookout record to CLASS: Surname, Given Name, Place of Birth (POB), Date of Birth (DOB), Refusal Site, Refusal Date and Refusal Code. When the Add is successful, a message appears reporting the Unique ID added to the database. Certain records, those containing a reason code + subcode for fraudulent claims to citizenship, are also copied to the Visa Lookout database.

Clicking the Delete link on a Name check display or Lookout list causes the Passport Delete page to display in a new window, filled by data from the selected record. The WebCLASS user must review the data that is in the record they wish to delete and click the “Yes” button. Clicking “No” returns the user to the previous display.

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. It does use information regarding individuals collected from government agencies involved in law enforcement,

national security, and U.S. border protection. The information is used to support the visa and passport issuance process.

d. Are contractors involved in the uses of the PII?

CLASS is owned by the Department but is operated and maintained by government contractor personnel. Contractors are involved with the design, development, and operation of the system. All users were required to pass annual computer security/privacy training and to sign non-disclosure and rules of behavior agreements.

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 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 Department personnel. In addition, access to the server rooms is protected by an electronic entrance combination lock as prescribed by internal Department policy.

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

Operations/Production staff supports CLASS production, data quality, and Pilot 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.

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 Department of State 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

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.

Visa applications are retained in compliance with the Visa Lookout Accountability provisions of the Illegal Immigration Reform and Immigration Responsibility Act of 1996 and the records disposition schedule. The complete disposition schedule for visa records is specified in the U.S. Department of State Records Disposition Schedule,

Chapter 14: Visa records, approved by the National Archives and Records Administration.

The retention of passport records varies depending upon the specific kind of record. Files of closed cases are retired and destroyed in accordance with the published record disposition schedules of the Department of State and the National Archives and Records Administration (NARA).

Disposition procedures are documented at the Office of Freedom of Information, Privacy and Classification Review, Room 1239, Department of State, 2201 C Street NW, Washington, DC 20520-1239.

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

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging.

The privacy risks are mitigated through the controlled access and rules of behavior that govern the users of CLASS throughout the lifetime of the data. Accuracy of the data is verified as described in section 3(d) above. Department of State OpenNet security protocols are used to ensure that the data is stored and backed up in a secure environment. Access to computerized files is password-protected and under the direct supervision of the system manager.

All physical records containing personal information are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

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 Department consular officers, domestic passport adjudication personnel, and attorneys who may be handling a legal, technical or procedural question resulting from an application for a U.S. visa or passport. CLASS shares an internal connection with the Consular Consolidated Database (CCD) and directly through the Front End Processor (FEP). CLASS shares information with the following systems internal to CA/CST:

Name of System	Type of Data	Data Flow
Non-Immigrant Visa (NIV)	Visa query	Bi-directional
American Citizen Services	Passport query	Bi-directional
Immigrant Visa Overseas (IVO)	Visa query	Bi-directional

Name of System	Type of Data	Data Flow
Visa Opinion Information Service (VOIS)	Visa query	Bi-directional
Waiver Review System (WRS)	Visa query	Bi-directional
Independent Name Check (INK)	Name check query	Bi-directional
Case Tracking System (CTS)	Name check query	Bi-directional
Passport Lookout Tracking System (PLOTS)	Name check query	Bi-directional
Travel Document Issuance System (TDIS)	Name check query	Bi-directional

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 CLASS External Interface (CXI) through various existing client applications that are routed through the Front End Processor (FEP), Telecommunications Manager (TCM), or Consular Consolidated Database systems, or through the CLASS interface known as WebCLASS (available to a limited number of Department authorized users) via OpenNet.

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. All physical records containing personal information are maintained in secured file cabinets or in restricted areas with access limited to authorized personnel. Access to electronic files is protected by passwords and is under the supervision of system managers. Audit trails track and monitor usage and access. Finally, regularly administered security/privacy training informs authorized users of proper handling procedures.

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

Any sharing of data, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. CLASS mitigates these vulnerabilities by working closely with the sharing organizations to develop secure standard operating procedures for using this data. These procedures are documented in sharing agreements such as the Memorandum of Understanding Between The Federal Bureau of Investigation and The United States Department of State for The Sharing of Records and Memorandum of Understanding Between the U.S. Customs Service and the Bureau of Consular Affairs for Use of the Treasury Enforcement Communications System (TECS) and for a Two-Way Exchange of Data within the Framework of the Interagency Border Inspection System (IBIS).

CLASS has formal, documented procedures to facilitate the implementation of its audit and accountability processes. The application produces audit records that contain sufficient information to establish what events occurred, the sources of the events

identified by type, location, or subject. System administrators regularly review and analyze the application audit records for indications of suspicious activity or suspected violations of security protocols.

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. User training is delivered annually in accordance with internal Department of State regulations. Access to CLASS is dependent on completion of a background investigation and an appropriate job need. Vulnerabilities and risks are mitigated through the system's certification process. NIST recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

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 via Consular Data Information Transfer System (CDITS):

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), Interpol is sent passport number updates from the U.S. Consular Lost and Stolen Passports (CLASP) database, which is a database within the CLASS system.

CLASS information is shared with the following agencies via Consular Consolidated Database (CCD):

Terrorist Screening Center (TSC) – TSC delivers Passport and Visa data to CLASS by way of a connection through the Consular Consolidated Database (CCD). 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 information was entered. This information is shared with TSC.

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.

National Counterterrorism Center (NCTC) – Monthly, CA/CST transmits the CLASP data file per NCTC's requirements that NCTC promptly review all USP information received and promptly delete the data if a reasonable belief that it constitutes terrorism information cannot be promptly established. For the purpose of CLASP data, NCTC will deem "promptly" as 90 days.

In addition, Lookout/Refusal data is transferred to CLASS from agencies external to the Department. These external agencies access CLASS via either the Consular Consolidated Database (CCD) or Consular Data Information Transfer (CDITS). Files are

transferred from the following agencies: Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS) Customs and Border Protection (CBP), DHS, Immigration and Customs Enforcement (DHS/ICE), Health and Human Services, Office of Child Support Enforcement (HHS/OCSE), U.S. Marshals Service, and the Department of Defense (DOD).

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 through CDITS and CCD.

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

Any data sharing, whether internal or external, increases the potential for compromising that data and creates new opportunities for misuse. CLASS mitigates these vulnerabilities by working closely with the sharing organizations to establish formal agreements and develop secure standard operating procedures for sharing the data.

Vulnerabilities and risk are mitigated through the system's certification process. NIST recommendations are strictly adhered to in order to ensure all appropriate data transfers and storage methods are applied.

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:

☒ contains information covered by the Privacy Act.

Provide number and name of each applicable systems of records:

- Visa Records, STATE-39
- 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?

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

Visa application forms provide a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court. This is outside the scope of CLASS.

The passport application form provides a Privacy Act Statement containing the authorities for collection of the information solicited on the form, purpose for soliciting the information, routine uses of the information solicited on the form and consequences of failure to provide information. This is outside the scope of CLASS.

Also, notice is provided in the System of Records Notice (SORN) Visa Records, State-39 and System of Records Notice (SORN) Passport Records, State-26.

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

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

Information is given voluntarily by the visa or passport applicant at the time they apply for services. Individuals who voluntarily apply for a U.S. visa or passport must supply all the requested information and may not decline to provide part or all the information required, if they wish to receive a visa or passport. The visa and passport application process are outside of the scope of CLASS.

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?

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

Applicants are advised on the use of the PII collected at the time they apply for a U.S. visa or passport. This is outside of the scope of CLASS.

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.

Notices provided in the SORNs regarding visa and passport records fully explain how the information may be used by the Department and how it is protected. The notice offered is reasonable and adequate in relation to the system's disclosed 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?

Data within CLASS is amended by authorized users at domestic passport agencies, U.S. embassies and consular posts overseas as well as approved domestic users within

the Information Management Liaison Division of the VO and the Passport Services Bureau. 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.

In addition, The Department will release the following information to a visa applicant upon request per guidance available to the public in 9 FAM 40.4:

1) Correspondence previously sent to or given to the applicant by the post;
2) Civil documents presented by the applicant; and
3) Visa applications and any other documents, including sworn statements, submitted by the applicant to the consular officer in the form in which they were submitted; i.e., with any remarks or notations by U.S. Government employees deleted.

CLASS information may also be protected in accordance with provisions of the Privacy Act of 1974 (5 U.S.C. 552a). Individuals may request access to or correction of their PII pursuant to FOIA or the Privacy Act, as appropriate.

Procedures for notification and redress are published in the Privacy Act SORN, and in rules published at 22 CFR 171.31 informing the individual regarding how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. Certain exemptions to Privacy Act provisions for notification and redress may exist for visa 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 171.36.

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?

There are only two types of direct users of CLASS: the CLASS Administrators who have access for the purpose of maintenance and production support and the users of WebCLASS who are authorized users approved by management within VO/I and PPT/IML. Both types of users are internal to the Department of State.

Direct access to CLASS for these user groups is limited to authorized Department of State users who have a justified need for the information in order to perform official duties, such as adjudicating visa or passport applications.

To access the system, persons must be an authorized user of the Department of State's unclassified network. Each authorized user must sign a user access agreement before

being given a user account. The authorized user's supervisor must sign the agreement certifying that access is needed to perform official duties. The user access agreement includes rules of behavior describing the individual's responsibility to safeguard information and prohibited activities (e.g. curiosity browsing). Completed applications are also reviewed and approved by the Information System Security Officer (ISSO) prior to assigning a logon. The level of access for the authorized user restricts the data that may be viewed and the degree to which data may be modified. A system use notification ("warning banner") is displayed before logon is permitted and recaps the restrictions on the use of the system. Activity by authorized users is monitored, logged, and audited.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. 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. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

CLASS also services Visa and Passport name check queries originating from users of client applications including NIV, IVO, VOIS, WRS, CCD, ACS, INK, TDIS and PLOTS, From the user workstation, these client systems pass their queries to CLASS via the Telecommunications Manager (TCM), Front End Processor (FEP), or CA's Enterprise Service Bus (ESB) depending on the type of transaction. Access to these client systems is addressed in each system PIA. The only non-Department access to CLASS is via CCD. Non-Department users who have access to the Independent Namecheck System (INK) via logon to CCD can conduct name check queries. Non-Department access to the CCD is addressed in the CCD PIA.

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.

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 deleted. Therefore, this level of privacy risk is negligible.

Additionally, system audit trails are available to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.) As a result of these actions, the residual risk is low.

11. Technologies

a. What technologies are used in the system that involve 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?

The Department of State operates CLASS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk and has implemented security controls. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, CLASS was certified and accredited for 36 months and is due to expire on May 31, 2011. This PIA is being submitted as part of the triennial certification and accreditation process. It is anticipated that the current C&A process will be completed in May 2012 resulting in a projected authorization to operate (ATO) date of May 31, 2015.