

Consular Lookout and Support System (CLASS) PIA

1. Contact Information

A/GIS/IPS Director
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Name of System: Consular Lookout and Support System

(b) Bureau: Consular Affairs (CA)

(c) System Acronym: CLASS

(d) iMatrix Asset ID Number: 558

(e) Reason for Performing PIA:

- New System
- Significant modification to an existing system
- To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable):

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

- Yes
- No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

CLASS currently has an Authority to Operate (ATO) which expires on November 30, 2018.

CLASS is a logical boundary that includes the following child systems in its ATO:

- eCLASS (child of CLASS) – ITAB 6578
- iCLASS (child of CLASS) – ITAB 5680

- CXI (child of CLASS) – ITAB 6579
- webCLASS (child of CXI) – ITAB 5679
- TCM (child of CLASS) – ITAB 564

As CLASS is referenced throughout this PIA, it is inclusive of all the child systems listed above.

(c) Describe the purpose of the system:

The Consular Lookout and Support System (CLASS) is used by Department of State passport agencies, posts, and border inspection agencies to perform namechecks on visa and passport applicants to identify individuals who may be ineligible for issuance or require other special action. In order for CLASS to operate, it relies on the following child systems:

- eCLASS and iCLASS are the namecheck search engines that use a normalized and indexed Oracle database along with an array of Intel-based servers and intelligent load balancers to achieve the required throughput. The eCLASS search engine performs namechecks against Lookout databases. iCLASS is currently used to vet eDV applicants and perform Consular Consolidated Database (CCD) lookup queries (citizen and visa data).
- CXI consists of various components that provide database interfaces with agencies outside of the State Department as well as Overseas and Domestic internal sources whereby these organizations can provide and receive updates to namecheck data.
- webCLASS is used to perform a required namecheck from any authorized user on a Department of State OpenNet machine through the website driven namecheck system.
- TCM is a software application that serves as a connection point (middle-tier) between Consular Affairs (CA) client systems and the namecheck system database, Consular Lookout and Support System (CLASS). TCM performs two main functions: translation and routing. TCM routes requests from CA client applications for visa namecheck transactions to CLASS and returns the response from the namecheck system databases to the CA client. Translation services ensure that transactions are delivered in the proper format to the destination system. Translation is necessary because the data format for CA clients and the namecheck system database differs.

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

With respect to U.S. passport application information maintained in CLASS, elements of PII collected and maintained include: 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.

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 8 U.S.C. 1101- 1504 (Immigration and Nationality Act (INA) of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541–1546 (Crimes and Criminal Procedure)
- 22 U.S.C 2651(a) (Organization of Department of State)
- 22 U.S.C. 211a–218 (Passports)
- Executive Order 11295 (August 5, 1966), 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)
- 26 U.S.C. 6039E (Information Concerning Resident Status)
- 22 C.F.R. Subchapter E, Visas
- 22 C.F.R. Subchapter F, Nationality and Passports

(f) Is the information searchable by a personal identifier (e.g., name or Social Security number)?

Yes, provide:

- **SORN Name and Number:** Overseas Citizen Services Records STATE-05, Passport Records STATE-26, and Visa Records STATE-39
- **SORN publication date (found under the Volume Number and above the Public Notice Number on the published SORN):**
 STATE-05: May 2, 2008
 STATE-26: March 24, 2015
 STATE-39: October 25, 2012

No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system?

Yes No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system?

Yes No

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.

State Department records in CLASS are covered by these records retention schedules:

A-14-001-02a Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: a. Case files on individual aliens **issued an immigrant visa**.

Disposition: Destroy 6 months after issuance.

DispAuthNo: N1-059-86-2, item 1a

A-14-001-02b Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: b. Case files on individual aliens **issued a non-immigrant visa**.

Disposition: Destroy 1 year after issuance.

DispAuthNo: N1-059-86-2, item 2b

A-14-001-02c(1)(a) Visa Case Files on Individual Aliens - Correspondence, memorandums, reports, forms, and other types of correspondence regarding individual visa applicants

Description: c. Case files on individual aliens **refused a visa**.

(1) Cases of living visa applicants.

(a) Cases of applicants refused or presumed ineligible on the basis of Sections 212(a) (1), (2), (3), (4), (5), (9), (10), (12), (13), (19), (22), (23), (27), (28), (29), (31), and (34) of the Immigration and Nationality Act.

Disposition: Retain until alien is 90 years of age or older, provided there has been no visa activity for the past 10 years, at which time destroy. (ref. NC1-59-86-2, item 3c1(a) and c1(c)).

DispAuthNo: N1-059-91-28, item 1c(1)(a)

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov.)

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

- Members of the Public
- U.S. Government employees/Contractor employees
- Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

Yes No

If yes, under what authorization?

Social security numbers are collected in Consular Affairs' systems in connection with visa and passport applications in accordance with 26 U.S.C. 6039E (Information Concerning Resident Status).

(c) How is the information collected?

Information maintained in CLASS is collected, in part, indirectly 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 is first provided by the applicant on one of the following Department of State passport or 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-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 is entered into other Department systems (listed below), and finally the information is transferred to CLASS for namecheck and lookout search purposes. If an applicant is refused a visa or passport, the information is forwarded to CLASS from the Visa or Passport Office after being scanned from the applicant's current passport and/or collected from the visa application form.

The Department of State's system sources include:

- Non-Immigrant Visa (NIV)
- Immigrant Visa Overseas (IVO)
- Consular Consolidated Database (CCD)
- American Citizen Services (ACS)
- Independent Namecheck (INK)

- Travel Document Issuance System (TDIS)
- Passport Lookout Tracking System (PLOTS)
- Tracking Responses and Inquiries for Passports (TRIP)
- Passport Information Electronic Records System (PIERS)
- Passport Records Imaging System Management (PRISM)
- Diversity Visa Information System (DVIS)

Information in CLASS may also be obtained independently of an application. Information may be forwarded from law enforcement entities and other government agencies, listed below, for inclusion in CLASS:

- 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)
- Social Security Administration (SSA)

(d) Where is the information housed?

- Department-owned equipment
- FEDRAMP-certified cloud
- Other Federal agency equipment or cloud
- Other

If you did not select “Department-owned equipment,” please specify.

(e) What process is used to determine if the information is accurate?

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 adjudication 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.

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

CLASS is constantly monitored and updated to ensure that it contains current information. An Operations/Production staff supports CLASS production, data quality, and Quality Assurance (QA) environments. The Operations/Production staff's primary responsibility is to monitor the production environment to ensure 24/7 availability of namecheck and refusal update submissions to users, and to ensure that replication updates between the redundant CLASS sites are current in accordance with State Department standards.

(g) Does the system use information from commercial sources? Is the information publicly available?

CLASS does not use information from commercial sources, and the information in CLASS is not publicly available.

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

Some, but not all, of the information that is included in CLASS is collected from the visa and passport applications submitted by individuals. However, the information submitted by the applicants on their applications is not directly added to CLASS. In other words, CLASS does not collect personal information directly from any individuals, and individuals do not have the opportunity or right to decline to have their information included in CLASS.

Individuals are not required to submit visa or passport applications, but the application forms themselves provide notice to individuals that their PII is being collected due to the information they would need to provide to complete the application.

Individuals are also on notice through the System of Records Notice (SORN) Visa Records, State-39 and System of Records Notice (SORN) Passport Records, State-26, that the information they provide in a visa or passport application is stored in a system of records.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information?

Yes No

If yes, how do individuals grant consent?

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

CLASS does not collect personal information directly from any individuals; therefore, the opportunity and/or right to decline options do not apply to this system. The passport information displayed in CLASS is derived from other State Department applications that are covered by their own PIAs outside of the scope of CLASS. Furthermore, passport applicants are advised of the uses of their PII and have the option to decline before they

complete the application. If applicants decline to provide the information, however, the application may be rejected.

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

In order to minimize privacy concerns, CLASS stores the minimum amount of PII required to process a visa or passport namecheck query.

The CLASS namecheck algorithms require PII to provide accurate results to Passport and Visa officers. However the databases are protected by published Oracle security guidelines, utilizing strong authentication and IP address filtering. Additionally audit logs are reviewed, as required, for anomalies and unauthorized access. WebCLASS and Client systems provide additional auditing of system uses to detect inappropriate uses of the stored data.

5. Use of Information

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

Information is collected by passport agencies, U.S. embassies and consulates, and border inspection agencies to perform namechecks of visa and passport applicants in support of issuance processing and document verification. CLASS performs namechecks 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.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes No

(c) Does the system analyze the information stored in it?

Yes No

If yes:

(1) What types of methods are used to analyze the information?

Not applicable because the system does not analyze the information.

(2) Does the analysis result in new information?

Yes

No

Not applicable because the system does not analyze the information.

(3) Will the new information be placed in the individual's record?

Yes

No

Not applicable because the system does not analyze the information.

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it?

Yes No

Not applicable because the system does not analyze the information.

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

Internally Shared - CLASS information is shared with 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), Consular Affairs Enterprise Service Bus (CAESB), Front End Processor (FEP), and Consular Data Information Transfer System (CDITS). 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 (ACS)	Passport query	Bi-directional
Immigrant Visa Overseas (IVO)	Visa query	Bi-directional
Independent Namecheck (INK)	Namecheck query	Bi-directional
Passport Lookout Tracking System (PLOTS)	Namecheck query	Bi-directional
Travel Document Issuance System (TDIS)	Namecheck query	Bi-directional
Tracking Responses and Inquiries for Passports (TRIP)	Passport query	Bi-directional
Passport Information Electronic Records System (PIERS)	Passport and CLASP query	Bi-directional
Diversity Visa Information System (DVIS)	Visa query	Bi-directional
Passport Records Imaging System Management (PRISM)	Passport query	Bi-directional

Externally 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 purposes of CLASP data, NCTC deems "promptly" to be 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) What information will be shared?

- 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).

(c) What is the purpose for sharing the information?

The purpose is for agencies to verify eligibility of persons of interest in order to issue travel documents or to determine if other special action is required.

(d) The information to be shared is transmitted or disclosed by what methods?

The information is transmitted via encrypted methods within CCD and CDITS.

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

Internally, information is transmitted in XML format to CLASS External Interface (CXI) through various existing client applications that are routed through FEP, CCD, CAESB, CDITS or the CLASS user interface, 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 and privacy training informs authorized users of proper handling procedures.

Any data sharing, whether internal or external, increases the potential for compromising or misusing the data. 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.

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 need-to-know. Vulnerabilities and risks are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly followed in order to ensure appropriate data transfers and storage methods are applied.

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

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Any data sharing, whether internal or external, increases the potential for compromising or misusing the data. 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.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

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 Directorate. 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, such as airports, train stations, and border crossings.

In addition, the Department will release the following information to a visa applicant upon request per guidance available to the public in 9 Foreign Affairs Manual 40.4 Note 5.3 (9 FAM 40.4 N5.3):

- 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 the Freedom of Information Act (FOIA) or the Privacy Act, as appropriate.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

Yes No

If yes, explain the procedures.

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.

Procedures for individuals to correct inaccurate or erroneous information are available to the public and published in the Privacy Act, SORNs STATE-05, STATE-26, and STATE-39 and in rules published at 22 CFR 171 Subpart D, Privacy Act Provisions informing individuals 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 171.26.

If no, explain why not.

(c) By what means are individuals notified of the procedures to correct their information?

Refer to section 7b.

8. Security Controls

(a) How is the information in the system secured?

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.

(b) Describe the procedures established to limit access to only those individuals who have an “official” need to access the information in their work capacity.

There are only two types of direct users of CLASS. CLASS Administrators have access for the purpose of maintenance and production support. The users of webCLASS are authorized users approved by management within the State Department.

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 and privacy training is required for all authorized users including security training and regular refreshment training.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

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.

(d) Explain the privacy training provided to authorize users of the system.

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.

- (e) **Are any security controls such as encryption, strong authentication procedures, or other controls in place to make the information unusable to unauthorized users?**

Yes No

If yes, please explain.

Security controls such as encryption and authentication procedures have been implemented in accordance with State Department policy and NIST guidelines.

- (f) **How were the security measures above influenced by the type of information collected?**

The information stored in CLASS was categorized using NIST's Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-60 revision 1. As a result of that categorization, the security measures outlined above were determined to be appropriate.

9. Data Access

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

The Operations/Production staff has access to CLASS data in the production, data quality, and Quality Assurance (QA) environments. Developers only have access to the QA environment of CLASS.

- (b) **How is access to data in the system determined?**

Access is determined on a "Need to Know" basis based on job requirements.

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

Yes No

- (d) **Will all users have access to all data in the system or will user access be restricted? Please explain.**

All users do not have access to all data within CLASS. Role-based access control is implemented to restrict access to CLASS data based on a user's need to know.

- (e) **What controls are in place to prevent the misuse (i.e. unauthorized browsing) of data by users having access to the data?**

Role-based access control is implemented to restrict access to CLASS data. Additionally, all user actions are audited and reviewed in accordance with State Department policy.