Consular Lookout and Support System (CLASS) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information 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 June 30, 2019.

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

- Enterprise CLASS (eCLASS); iMatrix 6578
- Interface CLASS (iCLASS); iMatrix 5680
- CLASS External Interface (CXI); iMatrix 6579

- webCLASS; iMatrix 5679
- Telecommunications Manager (TCM); iMatrix 564

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

(c) Describe the purpose of the system:

The Consular Lookout and Support System (CLASS) supports the Bureau of Consular Affairs mission requirements in assisting decisions for visa and passport issuance and to help establish a person's eligibility for overseas services. CLASS is used by Department of State passport agencies, posts, and Department of Homeland Security and other 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. Information is checked via the CLASS Consular Lost and Stolen Passports (CLASP) services component in support of border security. CLASS sends and receives visa lookout data and lists of lost, stolen, and revoked passports to and from various external agencies. 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 electronic Diversity Visa (eDV) applicants and perform Consular Consolidated Database (CCD) lookup queries (citizen and visa data). eCLASS and iCLASS share the same application code base.
- 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 the Department of State OpenNet system through the website driven namecheck system.
- Telecommunications Manager (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:

PII transmitted includes:

- Names of individuals
- Birthdates
- Personal Address
- Country or place of birth
- Gender
- Aliases
- Passport number
- Alien registration number (aliens only), national ID (aliens only)
- Social Security Numbers (SSN)
- Physical description
- Financial Information

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

- 5 U.S.C. 552a (Privacy Act of 1974 as amended)
- 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)
- 22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)
- 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 and Other Overseas 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: September 8, 2016
  STATE-26: March 24, 2015
  STATE-39: June 15, 2018

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

B-09-002-01a to B-09-002-40b: Consular Records Visa Services
Description: Information obtained from issued immigrant and non-immigrant visa application forms (DS-156, 157, 158, 160, 230, 260, and INS related forms I-129B,I-129F, I-130, I-140 and I-600) and supporting documentation. Immigrant visa case records potentially include the following types of case level data: unique identifier; applicant personal and biographic data; adjudication data; visa class information; visa clearance and name check data; case summary data; case status data; notes; and reports.
Disposition: Consular Records Visa Services records range from retaining up to 100 years to until superseded, obsolete, or no longer needed depending, on the type of record.

A-14-001-24 Name Check System
Description: Name Check History Master. This series contains a yearly listing of requests by Passport and Visa Office personnel to query the Passport and Visa Lookout systems. The listing provides statistical data for Bureau of Consular Affairs.
Disposition: Destroy when active agency use ceases.
DispAuthNo. NC1-059-83-04

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 passport applications in accordance with 26 U.S.C. 6039E (Information Concerning Resident Status). Social security numbers are also included in lookout data as part of data received from external government agencies, i.e. Federal Bureau of Investigation

(FBI), Health and Human Services (HHS), Internal Revenue Service (IRS), and US Marshal Service (USMS).

(c) How is the information collected?

Information processed by CLASS is from 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
- Form DS-160: U.S. Department of State Online Nonimmigrant Visa Application
- Form DS-1648: U.S. Department of State Online Application for A, G, or NATO Visa
- Form DS-260: U.S. Department of State Online Immigrant Visa and Alien Registration Application
- Form DS-261: U.S. Department of State Choice of Address and Agent
- Form DS-5501: Electronic Diversity Visa (eDV) Application
- Form DS-11: Application for a U.S. Passport
- Form DS-82: U.S. Passport Renewal Application for Eligible Individuals
- Form DS-5504: Application for a U.S. Passport - Name Change, Data Correction, and Limited Passport Replacement
- Form DS-64: Statement Regarding Lost or Stolen Passport

Data from these forms is entered into other Department systems (listed below), where 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)
- Internal Revenue Service (IRS)

(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 completing the applications for services. However, information is also checked against various Consular Affairs databases to determine any discrepancies. The CLASS Operations team ensures replication updates between the redundant CLASS sites are current to acceptable standards. Included in the submission of updates to/from CLASS are external agency feeds in which information is cross checked with internal Consular Affairs databases. External agencies providing information to the State Department are responsible for the accuracy of the information in the records that the agency submits to CLASS.

(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 by continuously checking against other databases and information provided by external agencies. 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?

CLASS does not collect personal information directly from any individuals. Information is provided from other internal databases and from external agencies.

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.

Individuals are not required to submit visa or passport applications; however, the application forms themselves addressed in paragraph 4(c), provide notice to individuals that their personally identifiable information (PII) is being collected due to the information required to complete the application for the requested services.

Individuals are also provided notice through the System of Records Notice (SORNs) for Overseas Citizen Services Records and Other Overseas Records, (STATE-05); Passport records (STATE 26); and Visa Records, (STATE-39) 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 transmitted by CLASS is derived from other State Department applications that are covered by their own Privacy Impact Assessments (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, 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 PII items collected by these systems are the minimum necessary to perform the actions required by this system. Concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the systems to perform the functions for which they are intended.

5. Use of Information

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

The CLASS system uses the information to perform namechecks of visa and passport applicants against various Consular Affairs databases 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

The CLASS system collects the information for the State Department's Visa and Passport Programs to perform name checks and to validate applicants' information. The collection supports visa and passport application submissions, processing, and approval/denial decisions.

(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 Consular Lost and Stolen Passports (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 and foreign governments:

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):

Customs and Border Protection (CBP) TECS System – 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 US citizens and legal permanent resident information received and promptly deletes 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.

Canada Beyond the Border (BtB) – CLASS provides a service that allows the Immigration Refugees and Citizenship Canada (IRCC) to run namechecks against CLASS and receive a filtered response, that includes information on foreigners of mutual interest to the US and Canada. No US Citizen data is included in the data exchange.

Federal Bureau of Investigation (FBI) Brady Act – CLASS sends a list of persons who have renounced US citizenship to the National Instant Criminal Background Service (NICS)

In addition, Lookout/Refusal data is transferred to CLASS from agencies external to the Department. Files are transferred from the following agencies: Drug Enforcement Agency (DEA), Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS), 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, Terrorist Screening Center (TSC), and the Department of Defense (DoD).

(b) What information will be shared?

- Names of individuals
- Birthdates
- Personal Address
- Country or place of birth
- Gender
- Aliases
- Passport number
- Alien registration number (aliens only), national ID (aliens only)
- Social Security Numbers (SSN)
- Physical description
- Social Media account indicators

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

The purpose of sharing information is to assist in determining eligibility for overseas services for visas and passports and to help establish a person's eligibility for overseas services. Sharing of information also supports border control security and services by providing visa lookout data and lists of lost, stolen, and revoked passports to and from various external agencies.

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

The information is transmitted by secured encrypted internal methods within CCD and CDITS. All of these activities and systems reside on the Department's secure intranet network, OpenNet. Information shared externally is exchanged through the CCD/ESB and CDITS, utilizing connection security and agreements. Additionally, shared data is transmitted via secure file upload.

CXI consists of various components that provide database interfaces with agencies outside of the State Department as well as overseas. The information is transmitted by secured encrypted internal methods in accordance with the Department of State Security guidelines.

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

Internally, information is transmitted in Extensible Markup Language (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. Access to electronic files is protected by inherited security controls from the

Department of State domain infrastructure. All accounts are 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?

Privacy concerns regarding the sharing of information in these systems focuses on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:
   Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need-to- know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft or information to non-authorized parties regardless of whether the motivation was monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII (which is Sensitive but Unclassified), and all higher levels of classification, and signing a user agreement.

2) Strict role-based access control, based on approved roles and responsibilities, authorization, need- to-know, and clearance level.

3) System authorization and accreditation process along with continuous monitoring via Risk Management Framework (RMF). Security controls are implemented for management, operational, and technical functions regarding separation of duties, least privilege, auditing, and personnel account management.

4) All communications shared with external agencies are encrypted as per the Department of State's security policies and procedures.

7. Redress and Notification

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

Applicants do not have access to their information on the CLASS system; however, procedures for access and redress are published in the System of Records Notices (SORNs) for Overseas Citizen Services Records and Other Overseas Records, (STATE-05); Passport Records (STATE-26) and Visa Records (STATE-39), and in rules published at 22 CFR 171 informing the individual how to inquire about the existence of records, how to request access to the records, and how to request amendment of a record. In addition, procedures are addressed during the review process of services requested via the source systems collecting the information.

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

☒Yes ☐No

If yes, explain the procedures.

Individuals can correct their information through the source system for the specified service requested in accordance with the prescribed guidance and processes. The updated information is captured in the CLASS system from the various source systems.

Additionally, procedures for individuals to correct inaccurate or erroneous information are available to the public and published in the 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?

Individuals are notified of the procedures to correct their information via the following ways:

1) During their interview for the specified service requested
2) Published SORNs as mentioned in paragraph 7b.
3) Instructions on forms and web pages (or links to Agency Privacy Policy)
4) Being notified by letter that a correction is needed.

8. Security Controls

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

The system is secured within the Department of State OpenNet where risk factors are mitigated through the use of defense in depth - layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

Access to applications is controlled at the application level with additional access controls at the database level. All accounts must be approved by the user's supervisor and the Information System Security Officer (ISSO). The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily. Data shared with other government agencies is carefully regulated according to a Memorandum of Understanding/Agreement (MOU/MOA) and an Information Security Agreement (ISA), formally signed by Authorizing Officers of each agency.

Applications are configured according the State Department Security Configuration Guides to optimize security while still providing functionality (complies with federal regulations and the Federal Information System Management Act (FISMA)). Applicable National Institutes of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during testing are reported appropriately and tracked until compliant or acceptably mitigated.

(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: administrators and authorized users. 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 to administer Consular Affairs services.

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 (OpenNet), which requires a background investigation and an application approved by the supervisor and Information System Security Officer. Each authorized user must sign a user access agreement/rules of behavior before being given a user account. Authorized users are issued a Personal Identity Verification/Access Card (PIV/CAC) and Personal Identification Number (PIN) which meets the dual authentication requirement for federal systems access and that is required for logon.

Access to the system is role-based and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists provide categories of information and reports that are to be restricted. Information System 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.

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

The CA System Manager and CA ISSO, in conjunction with CA Security team, periodically scan and monitor information systems for compliance with State Department Security Configuration Guides, conduct annual control assessments (ACA) to ensure that all systems/applications comply and remain compliant with Department of State and federal policies. Additionally, an array of configuration auditing and vulnerability scanning tools and techniques are used to continuously monitor the OpenNet-connected systems that host CA's major and minor applications for changes to the Department of State mandated security controls.

The execution of privileged functions (e.g. administrator activities) is included in the list of events that are audited. The data elements audited include: object created, object deleted, object modified, object rights modified, and custom access level modified.

CLASS applications are hosted on OpenNet servers. State Department Security Configuration Guide standards for OpenNet servers are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures. Remote connections are monitored using heuristic tools to detect suspicious traffic and malware as well as to restrict remote user capabilities.

In accordance with Department of State configuration guides, auditing is enabled to track the abnormal attempts and events on the host operating systems, and back-end database servers:

Operating System (OS)-Level auditing is set in accordance with the State Department Security Configuration Guides. The OS interface allows the system administrator or ISSO to review an audit trail through the Security Log found in the Event Viewer. In addition to the Security Log, the system log and application logs provide information on unauthorized events. The system log records events logged by the OS interface system components. The application log records events logged by applications. Audit logs may be derived from data such as event identifier, date, time, event type, category, user account, and computer name. Only the CA ISSO is authorized to generate and view security-related audit logs. Audit trails are reviewed weekly. Audit logs or records are maintained for at least one year.

- The OS interface-based auditing provides for some specific actions:
- Log-off – successes
- File access – failures
- Use of user rights – failures
- User/user group management – successes and failures
- Restart/shutdown/system security – successes and failures
- Process tracking – failure

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

In accordance with Department of State computer security policies, mandatory annual security/privacy training is required for all authorized users. Each user must complete the Cyber Security Awareness Training, which has a privacy component, annually and pass the Privacy Act PA-459 course, Protecting Personally Identifiable Information. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users sign that they agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy and integrity.

(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.

To combat the misuse of information by personnel, numerous management, operational and technical controls are in place in accordance with NIST 800-53 and Department of State Security Configuration Guides to reduce and mitigate the risks associated with internal sharing and disclosure. Data in transit is encrypted, physical and environmental protection is implemented, media handling configuration management is utilized and sanitization purge, destroy, shred, incinerate disposal methods are used. Boundary and information integrity protection including, but not limited to, firewalls, intrusion detection systems, antivirus software, and access control lists are in use. System and information integrity auditing are implemented to monitor and record possible attempts at

unauthorized access or data manipulation. All access to Department of State systems require dual factor authentication utilizing PIV/CAC and PIN.

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

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize that risk, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above were implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

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

Approved System Administrators have access to all components of the CLASS system to perform required maintenance, software updates etc. Authorized end-users have access to CLASS (via webCLASS) to conduct visa and passport inquiries and functions

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

Access is determined based on requests which are approved by the supervisor and ISSO. Access is role-based and the user is granted only the role(s) required to perform officially assigned duties.

(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.

Users other than the administrators will not have access to all data in the system. Separation of duties and least privilege is employed and users have access to only the data that the supervisor and ISSO approves to perform official duties.

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

-Access control policies and access enforcement mechanisms control access to PII. 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

-Separation of duties is implemented; access is role-based as required by policy.

-Least Privileges are restrictive rights/privileges or accesses needed by users for the performance of specified tasks and are implemented. Concerning PII, the Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

-Users are uniquely identified and authenticated before accessing PII (CAC/PIV and PIN), and activities while logged in can be traced to the person who performed the activity. Users are aware of this by reading and clicking 'I agree' to the logon banner.