PRIVACY IMPACT ASSESSMENT

Consular Lookout and Support System (CLASS)

1. Contact Information

A/GIS Deputy Assistant Secretary
Bureau of Administration
Global Information Services

2. System Information

(a) Date of completion of this PIA: May 2022
(b) Name of system: Consular Lookout and Support System
(c) System acronym: CLASS
(d) Bureau: Consular Affairs
(e) iMatrix Asset ID Number: 558
(f) Child systems (if applicable) iMatrix Asset ID Number: N/A
(g) Reason for performing PIA:

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

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

3. General Information

(a) Does the system have a completed and submitted data types document in Xacta?
☒Yes ☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) Is this system undergoing an Assessment and Authorization (A&A)?

☒Yes ☐No

If yes, has the privacy questionnaire in Xacta been completed?
☒Yes ☐No

(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 Consular Report of Birth Abroad (CRBA), visa issuances, and passport issuances and to help establish a person's eligibility for overseas services. CLASS performs searches (namechecks) against the visa and passport lookout databases (i.e., the databases that house records on persons who require further processing before issuance of a visa, passport, or an eCRBA document). CLASS

is used by Department of State (Department) passport agencies, posts, and Department of Homeland Security and other border inspection agencies to perform namechecks on CRBA, visa, and passport applicants to identify individuals who may be ineligible for issuances or require other special actions. CLASS sends and receives CRBA, 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 internal applications:

- eCLASS is a namecheck search engine that performs namechecks of U.S. persons and non-U.S. persons against visa and passport lookout databases internally within the CLASS database and within the Consular Consolidated Database (CCD).
- CLASS External Interfaces (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.

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

PII Transmitted on both U.S. persons and non-U.S. persons:
Name
Birth date
Birthplace
Gender
Address
Aliases
Passport number
Social Security Numbers (SSN)
Physical description
Financial information

Non-U.S. person PII only: Alien registration number and National ID number

(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)
- 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, etc.)?

☒Yes, provide:

SORN Name and Number: Visa Records, STATE-39
SORN publication date: November 8, 2021

SORN Name and Number: Passport Records, STATE-26
SORN publication date: March 24, 2015

SORN Name and Number: Overseas Citizen Services Records and Other Overseas Records, STATE-05
SORN publication date, September 8, 2016

☐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 Office 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.)

If yes provide (Consolidate as much as possible):

- **Schedule number: A-14-001-24, Namecheck System**
  Disposition Authority Number**:** NC1-059-83-04
  Length of time the information is retained in the system: Destroy when active agency use ceases.
  Type of information retained in the system**:** Namecheck History Master. This series contains a yearly listing of requests by Passport and Visa Office personnel to query the Passport and Visa Lookout databases. The listing provides statistical data for Bureau of Consular Affairs.

- **Schedule number: B-09-002-02b, Intermediary Records**
  Disposition Authority Number: DAA-GRS-2017-0003-0002(GRS 5.2, item 020)
  Length of time the information is retained in the system: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later. (Supersedes GRS 4.3 item 010; GRS

4.3, item 011; GRS 4.3, item 012; GRS 4.3, item 020; GRS 4.3, item 030; and GRS 4.3, item 031)
Type of information retained in the system**:** Immigrant Visa, Non-immigrant Visa, and Consular Consolidated Database hard copy and electronic input records, including applications, supplemental questionnaires, refusal worksheets and supporting or related documentation and correspondence, relating to persons who have been refused immigrant or nonimmigrant visas (including quasi-refusals), under the following section(s) of law: INA subsections 212(a)(1)(A)(i), (iii), and (iv); (2); (3); (6)(c), (e), and (F); (8); (9)(A) (if alien convicted of an aggravated felony), and (c); and 10(D) and (E); 222(g); Title IV of the Helms-Burton Act (22 USC 6021 et seq.); any cases requiring the Department's opinion code00 (Except quasi-refusal cases under (6)(c)(i)); INA subsection 212(a)(10)(c); Quasi-Refusals under 212(a)(6)(c)(i); 212(a)(9)(B); INA subsection 212(f); and Section 5(a)(1) of the Tom Lantos Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008. Also includes output records such as adhoc and other reports that contain summarized or aggregated information created by combining data elements or individual observations from a single master file or data base. Note: Applies to records covered by NARA Job No. N1-84-03-02, items 6, 7, 8, and 9.

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) On what other entities above is PII maintained in the system?

☐ Members of the Public
☐ U.S. Government employees/Contractor employees
☐ Other
☒ N/A

(c) If the system contains Social Security Numbers (SSNs), is the collection necessary?
☒Yes ☐No ☐N/A

- If yes, under what authorization?

26 U.S.C. 6039E (Information Concerning Residence Status)
22 U.S.C. § 2714a.(f) (Revocation or Denial of Passport in Case of Individual without Social Security Number)

(d) How is the PII collected?

Information processed by CLASS is from applicant submissions of paper or online passport, CRBA, and visa application forms via source systems which are received and processed at domestic passport agencies, U.S. embassies, and consulates overseas. Information is first provided by the applicant on one of the following Department of State 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
- Form DS-2029: Application for Consular Report of Birth Abroad of a Citizen of the United States of America
- Form DS-5507: Affidavit of Physical Presence or Residence, Parentage, and Support

Applications are completed via the source system or in person, and the information is then transferred via internal interface from the source system to CLASS for namechecks. Following are the CA source systems: Travel Document Issuance System (TDIS), Tracking Responses and Inquiries for Passports (TRIP) American Citizen Services (ACS), Non-Immigrant Visa (NIV), Passport Information Electronic Records System (PIERS), Passport Lookout Tracking System (PLOTS), Diversity Visa Information System (DVIS), Immigrant Visa Overseas (IVO) and the Electronic Consular Report of Birth Abroad (eCRBA). If an applicant is refused a visa or passport, the information is forwarded to CLASS from the Visa or Passport Office via the applicable source system.

Information may also be forwarded from law enforcement entities or other government agencies Drug Enforcement Agency (DEA), Terrorist Screening Center (TSC), Internal Revenue Service (IRS), United States Marshal Service (USMS), Department of Homeland Security (DHS), and Department of Defense (DoD), Health and Human Services (HHS), Federal Bureau of Investigation (FBI), Federal Bureau of Prisons (BOP)), for inclusion in CLASS inbound one way, via email, correspondence, or via one of the CA systems listed in paragraph 6a for inclusion in CLASS.

(e) 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.

(f) What process is used to determine if the PII is accurate?

Accuracy is the responsibility of the processes incorporated in the source system that originally collects the information. However, information is also checked against various Consular Affairs systems to determine any discrepancies. The CLASS team ensures replication updates between the redundant CLASS server sites are current. Included in the submission of updates to and from CLASS are external agency feeds in which information is cross checked with internal Consular Affairs systems. External agencies providing information to the Department are responsible for the accuracy of the information in the records that the agency submits to CLASS.

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

CLASS is constantly monitored and updated from various sources addressed in paragraph 4f above 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 systems and information provided by external agencies. The production environment is monitored to ensure 24/7 availability of namecheck and lookout update submissions, and to ensure that replication updates between the CLASS sites are current in accordance with Department standards.

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

No, CLASS does not use information from commercial sources, and the information in CLASS is not publicly available.

(i) How was the minimization of PII in the system considered?

In order to minimize privacy concerns, CLASS stores the minimum amount of PII required to process namecheck queries. The PII listed in 3d 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 and assessed during the system design and security configuration. Impact is minimized as collection of PII is limited to only what is required for the system to perform the function for which it was intended.

5. Use of information

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

The CLASS PII is used to assist in determining eligibility for passport, CRBAs, and visas, and to help establish a person's eligibility for overseas services by conducting namechecks against various systems. The PII used for namechecks lessens the threat of issuing passports or visas to individuals who are ineligible or require other special actions.

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

Yes, the PII is used to validate eligibility and to conduct namechecks on applicants applying for passports, CRBA, and visa services to identify those who may be ineligible or require special actions.

(c) Does the system analyze the PII stored in it? ☐Yes ☒No

If yes:

(1) What types of methods are used to analyze the PII?
(2) Does the analysis result in new information?
(3) Will the new information be placed in the individual's record? ☐Yes ☐No
(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

(d) If the system will use test data, will it include real PII? ☒Yes ☐No ☐N/A
If yes, please provide additional details.

PII is used in testing to improve the CLASS namecheck processing capability. Algorithms are designed to create additional searches against the data, considering how Department users adjudicating CRBAs, visas, and passports enter biographical data when running queriers, versus how the data sources entered CLASS data and records. A small set of PII is used to develop and/or adjust namecheck algorithms considering the data being queried in CLASS. The new or adjusted algorithms are tested to verify quality of namecheck hits and query response times. Once testing is complete the PII used is deleted. Databases with PII are encrypted and set up with access limited to designated CLASS team members approved by the supervisor.

6. Sharing of PII

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

Internal: The term "internal sharing" traditionally refers to the sharing of information within the Department of State (Department) but external to the owning organization (referred to as "bureau" at the Department of State. However, since the various Bureau

of Consular Affairs offices have unique processes and systems that are often interconnected, there are internal sharing routines and procedures in place within the bureau.

With that understanding, information in CLASS will be shared internally with the Front End Process (FEP), Consular Affairs Enterprise Service Bus (CAESB), Consular Consolidated Database (CCD), TDIS, TRIP, ACS, NIV, PIERS, PLOTS, INK, Consular Data Information Transfer System (CDITS), DVIS, IVO and eCRBA.

External: Information is shared externally with Treasury Enforcement Communication System (TECS), Beyond the Border (BtB), International Criminal Police Organization (Interpol), and American Institute of Taiwan.

(b) What information will be shared?

Internal: PII in paragraph 3d is shared with the CA systems listed in paragraph 6a.

External: PII in paragraph 3d is shared with the external systems and agencies listed in paragraph 6a.

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

The Information in paragraph 3d is shared with CA systems and agencies in paragraph 6a to conduct and provide namecheck assessments. The information is provided to the Department's consular posts, passport agencies, and external agencies for use in evaluating eligibility of CRBA, visa and passport applicants and other necessary actions for entry into the U.S.

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

Internal: Information is shared database to database by Department approved secure transmission methods for the handling and transmission of sensitive but unclassified (SBU) information. Information is also shared via encrypted email files upload to the CLASS support mailbox. Electronic files require entry via a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN), which meets the dual authentication requirement for federal systems access that is required for logon. Employee PIV/PIN access is approved and controlled by managers. Audit trails track and monitor usage and access.

External: The information is transmitted by secured encrypted methods according to the Department's Bureau of Diplomatic Security Configuration Guides. Information shared externally is exchanged using agreed upon security connection agreements and use of the information. Secure transmission methods are implemented, including encryption using Hypertext Transfer Protocol Secure (HTTPS) and secure communications using Transport Layer Security and multiple Transmission Control Protocol/Internet Protocol (TCP/IP) layers. These are permitted by internal Department

of State policies for handling and transmission of sensitive but unclassified (SBU) information. In a few cases, shared data is transmitted via secure encrypted password protected email files from external sources.

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

Internal: 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. Audit trails track and monitor usage and access. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

External: Safeguards in place for external sharing arrangements include memorandums of understanding with the various agencies and entities, on the security, use, and transmission of PII.

7. Redress and Notification

(a) Is notice provided to the record subject prior to the collection of his or her information?

CLASS is not a public facing system and does not collect information from the public. CLASS information is obtained from other CA source systems and external agencies. When the collection of information by the source system involves potential PII collected on U.S. citizens, there is a Privacy Act Statement displayed on the form in which the applicant is seeking a consular service, such as a passport. It is the responsibility of other agencies to provide notice to U.S. citizens when collecting PII.

(b) Do record subjects have the opportunity to decline to provide the PII or to consent to particular uses of the PII?
☐Yes ☒No

If yes, how do record subjects grant consent?

CLASS does not collect information from the public, but instead pulls information from CA systems and information submitted by agencies to conduct namechecks. Consent is acquired via the CA source system or agency where the applicant applies for services.

If no, why are record subjects not allowed to provide consent?

(c) What procedures allow record subjects to gain access to their information?

The published SORNs STATE-39, Visa Records; STATE-26, Passport Records; and STATE-05, Overseas Citizen Services Records and Other Overseas Records, include procedures on how to contact an office or individual for assistance with accessing or inquiring about the existence of records pertaining to the individual.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?
☒Yes ☐No

If yes, explain the procedures.

CLASS is not a public facing system. Consequently, individuals must follow processes of the source system to request correction of information. Individuals can also follow the record access procedures in SORNs STATE-39, STATE-26, and STATE-05, which include procedures on how to contact an office for assistance with addressing inaccurate information.

If no, explain why not.

(e) By what means are record subjects notified of the procedures to correct their information?

CLASS does not collect PII from individuals. The Department informs applicants on how to correct the information during their visa and passport adjudication processes. Also, emails are sent to applicants when there are inconsistencies so the applicant can provide correct information. Individuals can also follow procedures outlined in SORNs STATE-39, STATE-26 and STATE-05 to acquire points of contact information to correct information.

8. Security Controls

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

CLASS is secured within the Department of State intranet where risk factors are mitigated using 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 CLASS is controlled at the system level with additional access controls at the application level and requires a Personal Identity Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN). This meets the dual authentication requirement for federal systems access that is required for logon. All accounts must be approved by the user's supervisor and the Information System Security Officer. The audit vault is used to monitor all privileged access to the system and violations are reported to senior management daily.

CLASS is configured according to the Department's Bureau of Diplomatic 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.

(b) Explain the different roles that have been created to provide access to the system and the PII (e.g., users, managers, developers, contractors, other).

Access to CLASS is role-based and the user is granted only the role(s) required to perform officially assigned duties approved by the supervisor. CLASS Database administrators (DBAs), CLASS System administrators and Department of State employees have access to information in the system to aid in processing namechecks on applicants submitting passport and visa applications. Access to CLASS information is based on the prescribed roles and duties approved by the supervisor.

(c) Describe the procedures established to limit system and data access to only those individuals who have an "official" need to access the information in their work capacity.

Access to CLASS is role-based and restricted according to approved job responsibilities and manager concurrence. Administrative access controls permit categories of information and reports that are to be restricted. Local Information System Security Officers (ISSO) determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function, manager's approval, and level of clearance.

(d) How is access to data in the system determined for each role identified above?

In accordance with Department of State policy, CLASS employs the concept of least privilege for each user by allowing only authorized access to information in the system necessary to accomplish assigned job and tasks. All roles have been analyzed to determine the specific data set and corresponding functions required to accomplish assigned tasks in accordance with the person's job and level of security approved by the supervisor. Accordingly, when a user or service account is added to a particular database role, access is limited to only the data and functions allotted.

Access to CLASS is role-based and structured according to official job responsibilities and approval by the supervisor/manager. The user is granted only the role(s) required to perform officially assigned duties.

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

The CLASS audit service on its servers captures logs, access attempts, and all actions, exceeding the Department of State requirements. Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information in

CLASS. Monitoring occurs from the moment an authorized user attempts to authenticate to the Department of State OpenNet and respective applications. From that point on, any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after-hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system.

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

☒Yes ☐No

The CLASS System Security Plan includes information and procedures regarding access to data in CLASS.

(g) Explain the privacy training provided to each role identified in 8(b) that has access to PII other than their own.

All system administrators must take the IA210 System Administrator Cybersecurity Foundations Course which has a privacy component. In accordance with Department of State computer security policies, mandatory security training (PS800 Cyber Security Awareness) is required for all authorized users. Each user must annually complete the Cyber Security Awareness training, which has a privacy component, to access or use systems. Additionally, all Department of State personnel are required to take the course PA318 Protecting Personally Identifiable Information biennially. The Department's standard "Rules of Behavior" regarding the use of any computer system and the data it contains require that users agree to the rules and that they must protect PII through appropriate safeguards to ensure security, privacy, and integrity.