PRIVACY IMPACT ASSESSMENT

Independent Namecheck (INK)

1. Contact Information

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

2. System Information

(a) Date of completion of this PIA: December 14, 2021
(b) Name of system: Independent Namecheck (INK)
(c) System acronym: INK
(d) Bureau: Consular Affairs (CA/CST)
(e) iMatrix Asset ID Number: 29
(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):

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 Independent Name Check (INK) system allows posts to process namecheck queries (lookouts) on foreign nationals as part of the visa application process. The INK system allows users to add lookouts (independent checks and queries using the Consular Lookout and Support System (CLASS)) to check information, create refusal files, back scan existing refusal files, extract photos from the scanned documents to store as a separate scanned image associated with an INK system record, and generate reports. The INK system displays the namecheck results returned from CLASS.

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

The INK system collects the following information from Non-U.S. citizens:

- Name
- Aliases
- Phone number
- Address
- Birthdate
- Place of birth
- Photo (e.g., passport, national ID)
- Nationality
- Passport numbers
- National identification (ID) numbers.

Records in the INK system may contain PII about U.S. citizens or legal permanent residents who may be a sponsor, employer, representing agent, or a person who is associated with the non-U.S. citizen. The following PII may be collected on U.S. citizens:

- Name
- Address
- Phone number
- Email address.

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

- 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)
- 8 U.S.C. 1151-1363 (Title II of the Immigration and Nationality Act of 1952, as amended)
- 8 U.S.C. 1401-1504 (Title III of the Immigration and Nationality Act of 1952, as amended)
- 22 U.S.C. 2651a (Organization of Department of State)
- 22 U.S.C. § 3927 (Chief of Mission)
- 26 U.S.C. 6039E (Information Concerning Residence Status)
- 22 C.F.R. Parts 40-42, and 46 (Visas)
- 8 U.S.C. 1701 et seq., Enhanced Border Security and Visa Entry Reform Act
- U.S.C. 1101-1504 (Immigration and Nationality Act of 1952, as amended, Titles I-III, General, Immigration, Nationality and Naturalization)

- 8 U.S.C. 1701 et seq., Enhanced Border Security and Visa Entry Reform Act

(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

☐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

Disposition Authority Number: NC-059-83-04, item 23

Length of time the information is retained in the system: Destroy when active agency use ceases.

Type of information retained in the system: 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 (see items 1400020 and 1400210. The listing provides statistical data for the Bureau of Consular Affairs.

Schedule number: A-14-001-21

Disposition Authority Number: NC1-059-83-04, item 37

Length of time the information is retained in the system: Destroy when active agency use ceases.

Type of information retained in the system: This on-line series provides rapid access to names in the Visa Lookout Master. Searches may be by name, date of birth or visa office.

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?

(d) How is the PII collected?

The information in the INK system is transmitted and collected from CA systems (Consular Affairs Enterprise Service Bus (CAESB), Consular Shared Tables (CST), Consular Consolidated Database (CCD), Diversity Immigrant Visa Information System (DVIS), Immigrant Visa Information System (IVIS), Consular Lookout and Support System (CLASS), and Telecommunication Manager (TCM) systems) that provide visa services to foreign nationals as part of the visa application process. CA system information is transmitted database to database.

(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 of the information is conducted by quality checks against data transmitted via other internal CA systems for completeness, accuracy, and for inconsistencies at every stage of processing. Visa administrative policies and processes are also implemented, minimizing instances of inaccurate data.

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

Information is checked for currency at the point of collection of the source system, which the INK system checks information against, or during the in-person interview, where the applicant is requesting the specific visa service.

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

The INK system does not use information from commercial sources nor is the information publicly available.

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

The PII items listed in Question 3d are the minimum necessary to perform the actions required by the INK system. Concerns about collecting and maintaining PII 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 INK 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 PII is used for name checks and other searches to verify the identity of the applicant and to help determine if the applicant for a visa or refugee status is suitable for travel to the United States. Consular INK system personnel use the information to determine whether to issue the visa or refugee visa documentation.

(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 information collected is used to validate information provided against other CA systems and documentation to make determinations on the issuance of immigrant visas.

(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.

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 (DoS), but external to the owning organization (referred to as "bureau" at DoS). 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.

The INK system shares all PII information with the following CA systems: Consular Affairs Enterprise Service Bus (CAESB), Consular Shared Tables (CST), Consular Consolidated Database (CCD), Diversity Immigrant Visa Information System (DVIS), Immigrant Visa Information System (IVIS), Consular Lookout and Support System (CLASS), and Telecommunication Manager (TCM).

External: The INK system does not share information with external systems.

(b) What information will be shared?

Internal: The PII addressed in Question 3d is shared internally with the Consular Affairs systems listed above in paragraph 6a.

External: N/A

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

Internal: The PII in Question 3d is shared with the CA systems listed in Question 6a to process namecheck requests to screen, evaluate, and determine eligibility of visa applicants.

External: N/A

External: N/A

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

Internal: Information is shared database to database by secure encryption transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information.

External: N/A

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

Internal: The INK system safeguards entail secure protocol connections (Hypertext Transfer Protocol Secure (HTTPS)) which provides secure encryption interfaces. The Department of State security program involves the establishment of strict rules of behavior required by Department of State in place security controls for each major application, including the INK system. Periodic assessments are conducted on physical, technical, and administrative controls designed to enhance accountability, security of information, and data integrity. In addition, DoS employees must have a Personal Identity Verification/Personal Identification Number (PIV/PIN), as well as a separate unique user identification and password to access the INK system data. Data are transmitted within Department of State database to database.

External: N/A.

7. Redress and Notification

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

The INK system does not collect information directly from applicants. Respective notices are provided via the source systems collecting the information from applicants requesting the visa. Information is given voluntarily by the consenting applicants, by family members or the designated agent. Individuals are informed that failure to provide the information necessary to process the application may result in the application being rejected.

(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?

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

The INK system does not collect information directly from applicants, so individuals are not able to provide consent. Consent is granted at the point of collection for the source system where the immigrant visa application is being submitted.

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

System of Records Notice (SORN) STATE-39, "Visa Records" provides guidance and contact information regarding questions and procedures to access information.

(d) Are procedures in place to allow a record subject to correct inaccurate or erroneous information?

☒Yes ☐No

If yes, explain the procedures.

SORN STATE-39, "Visa Records", includes procedures on how to contact an office for assistance about the existence of records pertaining to the individual.

If no, explain why not.

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

SORN STATE-39, "Visa Records" provides information on procedures to access information and points of contact to inquire about information.

8. Security Controls

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

The INK system is secured within the Department of State intranet where risk factors are mitigated through 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 to perform official duties. Access to the INK system information is further protected with additional access controls set at the database level. All system accounts/access must be approved by the user's supervisor and the local Information System Security Officer.

The INK system is configured according to the State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 publication and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Internal access is limited to authorized Department of

State users, including cleared contractors who have a justified need to perform official duties.

(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).

(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.

Separation of duties and least privilege access are employed. Users have access to only the data that the supervisor and local Information System Security Officers (ISSOs) approve to perform official duties. Access is role-based and managed by access control lists, which restrict the user to only the role(s) required to perform officially assigned duties.

Least Privileges are restrictive rights/privileges or accesses users need for the performance of specified tasks. 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.

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

INK System Users: Depending on the role assigned, varying levels of access to data in the INK system are granted. The level of access is based on the position and role of the individual approved by the supervisor to perform the functions of processing namechecks to determine granting of visas. Access to the INK system is terminated when an INK system user leaves the assigned position.

System and Database Administrators: Individuals performing system and database functions have access to PII in the system due to the technical roles required to maintain and sustain operation of the system. Once an individual departs in one of these positions, their access to the INK system is terminated.

(e) What monitoring, recording, auditing safeguards, and other controls 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 Department of State Security Configuration Guides, conduct annual control assessments (ACA) to ensure systems 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 Department of State (DoS) OpenNet-connected systems that host CA's applications for changes to the DoS mandated security controls. Access control lists on the DoS OpenNet servers and devices, along with Department of State Security Configuration Guides standards are set up to restrict non-privileged users from disabling, circumventing, or altering implemented security safeguards/countermeasures.

In accordance with Department of State Configuration Guides, auditing is 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;
- Changes in file access restrictions.

The purpose of the audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data.

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

☒Yes ☐No

The INK System Security Plan (SSP) contains the procedures, controls and responsibilities regarding access to data in the system.

(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 State 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.