Privacy Impact Assessment (PIA): Independent Name Check (INK)

1. Contact Information

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

2. System Information

(a) Date PIA was completed: 07/22/2010

(b) Name of system: Independent Name Check

(c) System acronym: INK

(d) IT Asset Baseline (ITAB) number: 29

(e) System description:

The Independent Name Check (INK) system allows posts to process namecheck queries for foreign nationals independent of the U.S. visa application process, assist the Bureau of Population, Refugee and Migration (PRM) with screening, and the Kentucky Consular Center (KCC) with visa-related records management.

The INK system provides the following functionality:

1) The Namechecks function allows users to perform a namecheck query on an INK subject. Each query is submitted to CLASS. The query is also checked against the post's local database.

2) The Add Lookouts function allows users to send lookouts* to CLASS for INK subjects who have not yet applied for a visa. Lookout information may come from a variety of sources including newspapers, Department of Homeland Security (DHS) forms, letters, job applications, and lists of refugees.

3) INK allows users to create new category one (CAT-1) files and to backscan existing CAT-1 files (i.e., create electronic CAT-1 files from existing paper documents). At the Kentucky Consular Center (KCC), CAT-1 files can be created for multiple posts.

4) INK has the ability to scan supporting documentation, crop a photographic image from a scanned document, extract images from the scanned documents for storing as a separate scanned image associated with an INK record, and to generate and print a "hit" summary report on an individual.

5) INK also has the ability to manage multiple types of clearance requests. At this time, the system will only process Security Advisory Opinions (SAO) requests, which includes transmitting the request and processing responses received from the Consular Consolidated Database (CCD). In support of processing refugee cases, INK acts as a data transfer mechanism between the CCD and the Worldwide Refugee Admissions

Processing System (WRAPS). INK also has the capability to import and export SAO data in order to transmit and process SAO requests on foreign nationals.

*A lookout is a warning notice (or "hit") that a "hold" may exist. A "hold" is one of several types of entries stored in the Passport Namecheck System, indicating that a person may, by statute or regulation, be ineligible to receive a passport or other benefit of citizenship, or that a passport should be restricted.

(f) Reason for performing PIA:

- ☐ New system
- ☐ Significant modification to an existing system
- ☒ To update existing PIA for a triennial security re-certification
- ☐ PIA Information Review

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

(h) Date of previous PIA (if applicable): 11/15/08

3. Characterization of the Information

The system:

- ☐ Does NOT contain PII. If this is the case, you must only complete Section 13.
- ☒ Does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

INK primarily collects data on subjects who are foreign nationals independent of the U.S. visa application process and assists the Bureau of Population, Refugee and Migration (PRM) with screening and Kentucky Consular Center (KCC) with visa related records management. The information contained in INK is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

Because the subjects of the INK records are not U.S. persons (that is, U.S. citizens or legal permanent residents), they are not covered by the provisions of the Privacy Act and the E-Government Act of 2002. However, an INK record may contain PII about persons associated with the subject who are U.S. citizens or legal permanent residents. This PII data may include the following: employer name (whether foreign or domestic), sponsor name and address and U.S. contact name and phone numbers.

b. How is the information collected?

The visa applicant information is collected from the visa application, passport, corroborating documentation, in-person interviews and other sources such as newspapers, Department of Homeland Security (DHS) forms, letters, job applications, and lists of refugees. .

c. Why is the information collected and maintained?

The information is collected to determine the eligibility of foreign nationals who have applied or are applying for a visa to travel to the United States.

d. How will the information be checked for accuracy?

Accuracy of the information is the responsibility of the INK users (which includes the Department of State employees/contractors/customer service reps/consular officers overseas). Quality checks are done by reviewing the data input before submitting the namecheck query.

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

- Immigration and Nationality Act (INA) of 1952 (P.L. 82-414) and amendments
- Anti-Drug Abuse Act of 1988 (P.L. 100-690)
- Immigration Act of 1990 (P.L. 101-649)
- Illegal Immigration Reform and Immigration Responsibility Act of 1996 (P.L. 104-208)
- Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)
- Legal Immigration Family Equity "LIFE" Act (P.L. 106-553)
- USA PATRIOT Act of 2001 (P. L. 107-56)
- Enhanced Border Security and Visa Entry Reform Act of 2002 (P.L. 107-173)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The visa information collected by the visa application process is the minimum necessary to carry out the function of INK as identified in Section 3(c) above.

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

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

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

- **Insider threat.** This stems from internal employees or inadvertent human error to send PII over the internet.

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

- Inconvenience, distress, or damage to standing or reputation

- Financial loss
- Harm to Department programs or the public interest
- Unauthorized release of sensitive information
- Threats to personal safety
- Civil or criminal violation

In accordance with the Federal Information Security Management Act of 2002 (FISMA) and the information assurance standards published by the National Institute of Standards and Technology (NIST), there are management, operational, and technical security controls implemented to protect the data. These controls include regular security assessments, physical and environmental protection, encryption, access control, personnel security, identification and authentication, contingency planning, media handling, configuration management, boundary and information integrity protection (e.g., firewalls, intrusion detection systems, antivirus software), training, and audit reports.

4. Uses of the Information

a. Describe all uses of the information.

INK is used by Bureau of Consular Affairs (CA) personnel to retrieve namecheck results from CLASS, and to perform other searches to verify the identity of the applicant and to help determine if the applicant for a visa or refugee status is eligible for travel to the United States under applicable immigration laws and regulations. Consular and refugee personnel use the information to make a determination whether to grant each visa and refugee application. It is also used to enter lookout data.

b. What types of methods are used to analyze the data? What new information may be produced?

INK does not conduct analysis on the data collected from the visa application, other than verifying that the applicant is not on the lookout list. No data mining is used in INK.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Information collected by INK may come from newspapers, Department of Homeland Security (DHS) forms, letters, job applications, and lists of refugees. It is used to verify the visa applicant eligibility.

d. Is the system a contractor used and owned system?

INK is a government owned system. Government personnel are the primary users of INK. Some contractors use INK in support of the refugee process. Contractors are involved with the design and development of the system. All users were required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements.

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

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. The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the INK application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

All users, including external Agency users, are screened prior to their employment with the Department or their respective agency. The Bureau of Diplomatic Security (DS) is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before they are given access to the OpenNet and any CA/CST systems, including INK, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

CA officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard PII from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that contains PII.

5. Retention

a. How long is information retained?

Retention of records varies depending upon the type of record. Files of closed cases are retired and/or destroyed in accordance with the published Department of State and National Archives and Records Administration (NARA) record schedules. Some records, such as records of applicants who failed to make an appointment, are deleted after three years, while lookout records are retained until the subject is 100 years old and 10 years have passed since the last visa activity.

Paper records produced by this application are shredded or burned, per internal Department of State requirements for handling visas and Department of State record disposition schedules.

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

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

All physical records containing PII are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager.

When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

INK information is shared with authorized Department of State consular officers and staff that may be adjudicating visa or refugee cases or handling a legal, technical or procedural question resulting from an application for a U.S. visa or refugee status.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is shared by secure transmission methods permitted under Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. Security officers determine the access level an application user (including managers) may require depending on the user's particular job function and level of clearance. System managers and business owners are responsible for safeguarding the records processed, stored, or transmitted by INK.

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

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

Any sharing of data, whether internal or external, increases the potential for compromising the data and creates new opportunities for misuse. INK 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. Vulnerabilities and risk are mitigated through the system's certification process. National Institute of Standards and Technology (NIST) recommendations are strictly adhered to in order to ensure appropriate data transfers and storage methods are applied.

To reduce the privacy risks, access to information is controlled by application access controls. Every server on the CA OpenNet has NetIQ Security Manager installed and it is used to monitor server activity. Management Control Reports identify actions of authorized users and allow management to review daily activity. User training at the application level is delivered annually in accordance with internal Department of State regulations.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

INK does not provide any direct external connections to external agencies/organizations.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

Not applicable.

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

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

8. Notice

The system:

☒ Contains information covered by the Privacy Act.

Note: The information of the U.S. citizen or a legal permanent resident who is associated with the INK subject is cover by the Privacy Act.

Provide number and name of each applicable system of records.

(visit *www.state.gov/m/a/ips/c25533.htm* for list of all published systems):

- Visa Records. STATE-39

☐ Does NOT contain information covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice is provided to the individual throughout the visa application process.

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

Information used by INK was already provided voluntarily by the visa applicants when they applied for a U.S. visa.

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

Information used by INK was already provided by the applicants during the visa application process. They have no right to limit the use of the information to include namecheck.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

The information provided by the applicant is considered a visa record subject to confidentiality requirements under section 222(f) of the Immigration and Nationality Act (INA).

The information provided on the visa application form and in the SORN regarding visa records fully explains how the information may be used by the Department and how it is protected.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

The information in INK is considered a visa record subject to confidentiality requirements under INA 222(f). While information is not collected directly from visa applicants for specific use in INK, applicants are put on notice by information provided on the visa application forms and in the SORN regarding visa records that fully explain how information may be used by the Department and how it is protected.

The Department will release the following information to a visa applicant upon request and this guidance is available to the public in 9 FAM 40.4:

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

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

Procedures for notification and redress are published in the Privacy Act SORN cited in this PIA, and in rules published at 22 CFR 171.31. The procedures inform the individual about how to inquire about existence of records, how to request access, and how to request an amendment to 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 171.32.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

To the extent visa information in INK may be Privacy Act covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to

the system's stated purpose and uses and its applicable legal requirements. Therefore this category of privacy risk is appropriately mitigated in INK.

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Internal access to INK is limited to authorized Department of State users that have a justified need for the information in order to perform official duties. To access the system, the user must be an authorized user of the Department of State's unclassified network. Access to INK requires a unique user account assigned by a supervisor. 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. The Department of State's Consular Shared Tables (CST) application is used to maintain user accounts and user roles for the INK application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

b. What privacy orientation or training for the system is provided authorized users?

All authorized users of INK must pass computer security and privacy awareness training prior to receiving access to the system and must complete annual refresher training to retain access.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

To reduce any potential for residual risk related to system and information access, INK maintains strict access control lists, which define who can access the system, and at what privilege level. These lists are regularly reviewed, and inactive accounts are promptly terminated. Additionally, INK creates automatically generated audit trails that are regularly monitored and reviewed to deter and detect unauthorized uses. (An audit trail provides a record of which particular functions a particular user performed--or attempted to perform.)

11. Technologies

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

INK is a government off-the-shelf (GOTS) product that meets required security capabilities, approved design and development processes, required test and evaluation procedures and documentation under the supervision of a Project Manager in accordance with the Department of State internal policy. Additionally, INK receives input from Department of State security officers regarding any potential security issue(s).

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

No technologies that are known to elevate privacy risk are employed in INK.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department of State operates INK in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department of State has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. The Department of State performs routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, INK was certified and accredited for 36 months to expire on August 31, 2010.