Privacy Impact Assessment (PIA): Non-Immigrant Visa System (NIV)

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: 07/21/2010

(b) Name of system: Non-Immigrant Visa System

(c) System acronym: NIV

(d) IT Asset Baseline (ITAB) number: 65

(e) System description:

NIV provides automated support to the adjudication of a nonimmigrant visa application from individuals wishing to come to the United States for a temporary stay. NIV also provides for the administration of federal law and regulations that govern the issuance or refusal of nonimmigrant visas. NIV is a case record and maintenance application used at overseas posts to review, and complete the visa adjudication. The NIV System automates and streamlines the post's capabilities for:

1. Processing applicant, vessel, petition, referral, and diplomatic note data, capturing photos and fingerprints;
2. Name check hit results;
3. Viewing fingerprint Automated Biometric Identification system (IDENT) and Integrated Automated Fingerprint Identification system (IAFIS) clearance request results;
4. Viewing facial recognition clearance request results;
5. Recording the decision of the adjudicating officer;
6. Printing the Machine Readable Visa (MRV);
7. Scanning documents;
8. Processing Advisory Opinions and Security Advisory Opinions (SAO); and
9. Processing Admissibility Review Information Service (ARIS) Waivers.

(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): 12/03/2008

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?

NIV collects data on foreign nationals as part of the U.S. non-immigrant visa application process. The data on foreign nationals include name, address and telephone number, nationality, birth date, gender, birth country, passport number and passport issuance and expiration information and biometric data.

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

Because nonimmigrant visa applicants themselves 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 or the E-Government Act of 2002. However, an NIV record may include personally identifiable information (PII) about persons associated with the nonimmigrant visa applicant who are U.S. citizens or legal permanent residents.

This PII data on U.S. citizens may include the following: U.S. sponsor's name, address and phone number; U.S. contact name, address and phone numbers; and employer name, address and phone numbers. The source of information is the visa applicant, through petitions and visa applications.

b. How is the information collected?

The information is collected by consular posts overseas from visa applications (paper form or web via Electronic Visa Application Form (EVAF)), passports, corroborating documentation and in-person interviews and includes capture of fingerprints via Ten Print Live Scan (TPLS).

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 nonimmigrant visa to travel to the United States for a temporary purpose.

d. How will the information be checked for accuracy?

Accuracy of the information on a nonimmigrant visa application is the responsibility of the applicant and NIV users, which includes the Department of State employees/contractors/customer service reps/consular officers at posts. Quality control checks are done by reviewing the visa application to ensure that all required fields are complete and reflect accurate information before accepting the application.

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 personal data collected by NIV is the minimum necessary to carry out the function of NIV as identified in Section 3(c) above.

Due to the strict security controls required by all Department 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 are:

- **Device theft or loss** Lost or stolen laptops and other devices such as removable drives that 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** Disgruntled employees seeking revenge 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.

NIV is used by consular officers to record information for name checks, fingerprint matching, and other searches to verify the identity of the applicant and to help determine if the applicant is eligible for travel with a visa to the United States under applicable immigration laws and regulations. Consular officers use the information to make a determination whether to grant a non-immigrant visa.

Data can be retrieved in NIV by keyword searches, such as applicant name, visa foil number, case number, and/or by barcode scanning.

Issuance and refusal information is shared with the Department of Homeland Security (DHS) including name, DOB, gender, and visa information, such as issuance or refusal date and visa foil number.

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

NIV generates a variety of reports for management and accountability purposes.

The following is a list of management reports available in the system. Each report produces information for the date range specified.

Report Name	Report ID	End of Day	End of Month	Semi-Annual
Closed/Refused NIV Cases Without Associated Scanned Documents	77I	Y	Y	N
MRV Fees for Non-Immigrant Visas by Visa Class	FEE	N	N	N
NIV BCC Report - LCP Production Summary Report	BCC5	Y	Y	N
NIV Foils Unprinted/Deleted	77B	N	N	N
NIV Issuance Count Adjustments by Visa Class and Nationality	88	N	N	Y
NIV Overcome/Waivers by Grounds of Ineligibility	99	Y	Y	Y
Non-Immigrant Visa Applicant Case Accountability	CS2	N	N	N
Non-Immigrant Visa Cases by Referrer	11G	N	N	N
Non-Immigrant Visa Cases by Referrer That Were Waived	11P	N	N	N
Non-Immigrant Visa Lookout Actions Taken	33A	Y	N	N
Non-Immigrant Visa Referral Cases by Adjudicating Officer	11M	N	N	N
Non-Immigrant Visa Referral Cases by Approving Officer	11J	N	N	N
Non-Immigrant Visa Referral Cases Without Associated Documents	11Q	N	N	N
Non-Immigrant Visa Refusals	33	Y	Y	Y
Non-Immigrant Visa Refusals Overcome and Waiver Report	OW	N	N	N
Non-Immigrant Visa Tickler Report	11F	N	N	N
Non-Immigrant Visa Workload Summary	WL	Y	N	N
Non-Immigrant Visas by Applicant with No MRV Fees Paid	NOF	N	N	N
Non-Immigrant Visas Entered by Applicant Nationality	55A	N	N	N
Non-Immigrant Visas Issued and Refused by Applicant Nationality	55	Y	Y	N
Non-Immigrant Visas Issued and Refused by Referral Adjud Officer	11O	N	N	N
Non-Immigrant Visas Issued and Refused by Referral Approving Officer	11N	N	N	N
Non-Immigrant Visas Issued and Refused by Referrer	11H	N	N	N
Non-Immigrant Visas Issued and Refused by Visa Class	44	Y	Y	N
Non-Immigrant Visas Issued by Visa Class and Nationality	22	N	Y	Y
Status of Non-Immigrant Visas Entered	CS1	N	N	N

The following is a list of accountability reports generated by the system. Each report produces information for the date range specified.

Report Name	Report ID	End of Day	End of Month	Semi-Annual
BCC Cases with IDENT Hits	77G	Y	Y	N
Daily Non-Immigrant Visa Report - Visas Printed and Spoiled	VP	Y	N	N
NIV BCC Report - DHS Cards Spoiled for DHS Reprint	BCC1	Y	Y	N
NIV BCC Report - DHS Cards Spoiled for LCP Reprint	BCC4	Y	Y	N
NIV BCC Report - IDENT CHECK Report	BCC6	Y	Y	N

NIV BCC Report - LCP Cards Spoiled for LCP Reprint	BCC2	Y	Y	N
NIV BCC Report - QA List Report	BCC7	N	N	N
NIV BCC Report - Reentered/Recaptured	BCC3	Y	Y	N
NIV Issuances and Refusals for Host Country Applicants	11E	Y	Y	N
Non-Immigrant Visa Applicants Entered by Operator	11D	Y	Y	N
Non-Immigrant Visa Applicants Entered by Source Code	11L	Y	Y	N
Non-Immigrant Visa Cases Deleted	77F	Y	N	N
Non-Immigrant Visa Critical Fields Changed	77E	Y	N	N
Non-Immigrant Visas Approved and Refused by Adjudicator	11C	Y	Y	N
Non-Immigrant Visas Issued and Refused by Case Tag	CT	Y	N	N
Non-Immigrant Visas Issued Refused by Application Source	11B	Y	Y	N
Non-Immigrant Visas Reprinted	77A	Y	Y	N
Non-Immigrant Visas Spoiled	77C	Y	Y	N
Number of Machine Printed Non-Immigrant Visas	11A	Y	Y	N
Number of Machine Printed Non-Immigrant Visas by Foil Range	11K	N	N	N
Refusal Cases Inadvertently Not Sent to CLASS	77H	Y	Y	N
Refusal Cases Not Sent to CLASS	77D	Y	Y	N

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

Visa applicant data such as photo, fingerprint, proof of birth, birth place, other identifying documents, and existing passports, provided by visa applicants and/or foreign authorities is used to effectively identify the visa applicant and determine eligibility to travel to the United States.

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

NIV is a government owned system. Government personnel are primary users of NIV. Contractors are involved with the design and development of the system. Direct hire U.S. government employees have the sole responsibility for adjudicating NIV applications to determine if applicants are entitled for non-immigrant visa issuance. All employees and contractors are required to pass annual computer security/privacy training, and to sign non-disclosure and rules of behavior agreements. All contracts contain approved Federal Acquisition Regulation (FAR) Privacy Act clauses.

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 NIV application. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

All users, including external Department users, are screened prior to their employment with the Department. 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 system, including the NIV, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Consular 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?

Record retention varies depending upon the type of record. Files of closed cases are disposed in accordance with published Department of State record schedules as approved by the National Archives and Records Administration (NARA).

Some records/cases are kept on file for the purpose of determining eligibility as opposed to a data requirement. For example, 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 the NIV 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?

NIV 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 NIV.

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. NIV 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 Bureau of Consular Affairs (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?

NIV data is shared via data sharing arrangements. Applicant fingerprints, photo and personal data are sent to DHS for the purpose of checking the applicant's fingerprint information against DHS databases and establishing a record within DHS's Automated Biometric Identification (IDENT) system. NIV issuance data is forwarded to DHS for use at US ports of entry to verify the validity of the visa. NIV also transmits applicant fingerprints and personal data to the FBI fingerprint system for the purpose of checking to determine if the person has a criminal record that would have an effect on visa eligibility.

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

NIV data is replicated from the databases at each post to the Consular Consolidated Database (CCD). When the CCD receives fingerprint requests or visa issuance data, the CCD forwards the information to the Department's datashare applications. Each data sharing arrangement with federal agency partners is covered by a written agreement in the form of a memorandum of understanding or exchange of letters as well as technical documentation including an interface control document and interagency security agreement. Data is sent through encrypted lines.

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

NIV information is shared with U.S. government agencies with a statutory requirement and in accordance with confidentiality requirements under INA section 222(f). 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 any risk is addressed through the user-authorization process.

8. Notice

The system:

☒ Contains information covered 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?

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

The non-immigrant visa application form provides a statement that the information collected is protected by section 222(f) of INA. INA section 222(f) provides that visa issuance and refusal records shall be considered confidential and shall be used only for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States. Certified copies of visa records may be made available to a court which certifies that the information contained in such records is needed in a case pending before the court.

Also, notice is provided in the System of Records Notice Visa Records, State-39.

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

Information is given voluntarily by the applicants and with their consent, by family members and other designated agents.

Individuals who voluntarily apply for a U.S. visa must supply all the requested information, and may not decline to provide part or all the information required, if they wish visa services.

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?

Applicants may decline to provide information; otherwise, they have no right to limit the use of the information (consistent with the system's disclosed purposes and uses).

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 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 NIV is considered a visa record subject to confidentiality requirements under INA 222(f).

Visa applicants may change their information at any time prior to submission of the application to the post. Once that is done, applicants may make changes only by filing a new application with the Department or correcting the information during the course of a visa interview. 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
(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.

NIV information 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, and in rules published at 22 CFR 171.31 informing the individual regarding 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 171.32.

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

To the extent information in NIV may be Privacy Act-covered, the notification and redress mechanisms offered to individuals are reasonable and adequate in relation to the system's stated purposes and uses and its applicable legal requirements.

Therefore, this category of privacy risk is appropriately mitigated in NIV.

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 NIV is limited to authorized Department of State users, including contractors that have a justified need for the information in order to perform official duties. To access the system, a user must be an authorized user of the Department of State's unclassified network. Access to NIV 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 abstain from 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 NIV 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 users 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.

Access control lists, which define who can access the system, and at what privilege level, are regularly reviewed, and inactive accounts are promptly deleted. Additionally, system audit trails are regularly analyzed and reviewed to deter and detect any unauthorized activity. (An audit trail provides a record of all functions authorized users perform--or may attempt to perform.)

11. Technologies

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

NIV does not employ any technology known to elevate privacy risk.

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

Since NIV does not use any technology known to elevate privacy risk, standard robust safeguards are determined to be at the very minimum satisfactory in this application.

12. Security

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

The Department of State operates NIV 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 has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. The Department 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, NIV was certified and accredited for 36 months to expire on August 31, 2010.