

Non-Immigrant Visa System (NIV)

1. Contact Information

Department of State Privacy Coordinator

Margaret P. Grafeld
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

2. System Information

- (a) Date PIA was completed: December 3, 2008
- (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 to 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 visa types. 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)
- 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

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

PIA Information Review

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

(h) Date of previous PIA (if applicable): 04/25/2007

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 primarily 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 E-Government Act. However, an NIV record may include PII about U.S. citizens or legally permanent residents associated with the nonimmigrant visa applicant.

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

b. How is the information collected?

The information is collected from various sources such as visa application, passport, corroborating documentation and in-person interviews.

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. Quality checks are conducted against the submitted documentation at every stage and administrative policies minimize instances of inaccurate data.

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

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.

Due to strict security controls that are required to be in place before operation of the system, no identified privacy risks are associated with this system. The controls are subject to rigorous testing, formal certification and accreditation. Authority to operate is authorized by the Chief Information Officer (CIO) for DOS. Security controls are reviewed annually and the system is certified and accredited every three years or sooner if significant or major changes are made to the existing application. Only authorized users with a need to know are granted access to NIV.

4. Uses of the Information

a. Describe all uses of the information.

NIV is used to supply information for name checks, fingerprint matching, and other searches to verify the identity of the applicant and to help determine if the applicant is suitable for travel with a visa to the United States. Consular officers use the information to make a determination whether to grant an NIV. 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 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 statistical and management purposes.

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 provided by visa applicants and/or foreign authorities is used to effectively identify the visa applicant.

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

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

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 DoS record schedules as approved the National Archives and Records Administration.

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

All physical records containing personal information 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 DoS consular officers that may be handling a legal, technical or procedural question resulting from an application for a U.S. visa.

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 by internal DoS policy for the handling and transmission of sensitive but unclassified (SBU) information. An Interface Control Document (ICD) and Memorandum of Understanding (MOU) define

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

and disclose transmission format via OpenNet. 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.

Access to information is controlled by application access controls. 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 DoS 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 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 (MOU) 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

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

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).

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

The information provided on the form and in the SORN regarding visa records fully explain 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 Consulate or Embassy. 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

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

- 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 DOS users that have a justified need for the information in order to perform official duties. To access the system, authorized users must be an authorized user of the DOS' 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 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.

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

- 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

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

DoS 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. DoS has conducted a risk assessment of the system to identify appropriate security controls to protect against risk, and implemented controls. DoS 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.