

1. NATIONAL AUTOMATED IMMIGRATION LOOKOUT SYSTEM (NAILS)

Applicability: Agency-wide

Identifying Information:

Description: NAILS is a mission-critical online interactive application system that facilitates the inspection and investigation processes by providing quick and easy retrieval of biographical data or case data on individuals who may be inadmissible to the United States. The system contains the names and reference data on violators and suspected violators of the immigration statutes enforced by the DHS. The system has various search capabilities including soundex code and the records are indexed by names of individuals and record numbers. NAILS is a mainframe system located at the Department of Justice Data Center in Dallas, Texas and is available to users at headquarters, regional, administrative centers, service centers, district offices, ports of entry, and other file control offices and other offices of the DHS.

Specific Restrictions: NAILS contains highly sensitive personal information. All records in NAILS are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. The safeguards include restricting access to those with a need-to-know to perform their official duties, using locks and alarm devices, passwords and/or encrypted data communications. 5 U.S.C. § 552 prohibits the unauthorized release of data in NAILS.

Vital Record: Yes.

Specific Legal Requirements: 8 USC §1101, 8 USC §1185

Disposition Information:

- a. System inputs: Major inputs include on line entry of lookout records by users, final deportation orders from the Deportable Alién Control System (DACs), lookout records from the Detention and Deportation Branch, Non-Immigrant Information System (NIIS) [Visa Waiver and Guam Waiver Confirmed Overstay only], Department of State's Consular Lookout and Support System (CLASS), lost and stolen passport data from the National Lookout Unit, lookout records from the TIPOFF database (suspected terrorist database), and violators from the National Security Entry Exit Registration System (NSEERS) and the Student and Exchange Visitor Information System (SEVIS).

TEMPORARY. Destroy/Delete after the data has been transferred to the master file and verified.

- b. System data: Types of data elements include the record number, alien file number, name of the person and known aliases, date of birth, country of birth, country code, height, weight, race, eye color, hair color, nationality code, distinguishing marks, passport or seamen's book number, the office symbol which is automatically generated to identify the agency of the system user, the cancellation date which is derived from the justification, and the justification for establishing the record which is indicated by a case code that is determined by the nature of the violation(s), and if they are armed and dangerous.

(1) Complete system. Restrictions per 5 U.S.C. § 552.

PERMANENT. Fiscal year end data is permanent. Transfer a copy of the data to the National Archives and Records Administration in blocks of 5 fiscal years when the data is at least 10 years old in accordance with 36 CFR 1228.270.

(2) Public use version. Consists of redacted copy of 1b(1) with personal identifiers removed.

PERMANENT. Fiscal year end data is permanent. Transfer a copy of the data to the National Archives and Records Administration in blocks of 5 fiscal years when the data is at least 10 years old in accordance with 36 CFR 1228.270.

Note: The redacted version becomes obsolete when the unredacted version becomes public.

- c. System outputs: Records sent to the Interagency Border Inspections System (IBIS), Central Intelligence Agency (CIA), and various reports.

TEMPORARY. Destroy/delete when no longer needed for agency business.

- d. System documentation: Regardless of medium, record layouts, technical description of the file, data dictionaries, operational manuals.

PERMANENT. Transfer to the National Archives and Records Administration with system data as indicated in item 1b(1) and 1b(2) above.