Dated: July 20, 2006.

Eric B. Broderick,

Acting Deputy Administrator, Assistant Surgeon General, Substance Abuse and Mental Health Services, Administration.

[FR Doc. 06–6500 Filed 7–26–06; 8:45 am]

BILLING CODE 4162–20–M

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2006–0036]

System of Records

AGENCY: Office of the Secretary, DHS.

ACTION: System of records notice.

SUMMARY: The Department of Homeland Security is republishing the Privacy Act system of records notice for the Automated Biometric Identification System in order to expand its scope and authority to serve all or most programs that collect biometrics as part of their mission. As previously published, this system stored biometric information as a result of encounters pursuant to the Immigration and Nationality Act. As now proposed, this system will store biometric and limited biographic data collected for all national security, law enforcement, immigration, intelligence, and other mission-related functions.

DATES: Written comments must be submitted on or before August 28, 2006.

ADDRESSES: You may submit comments, identified by DOCKET NUMBER DHS–2006–0036 by one of the following methods:

- Federal e-Rulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Fax: (202) 298–5201 (not a toll-free number).
- Mail: Steve Yonkers, US–VISIT Privacy Officer, 245 Murray Lane, SW., Washington, DC 20538; Maureen Cooney, Acting DHS Chief Privacy Officer, Department of Homeland Security, 601 S. 12th Street, Arlington, VA 22202–4220.

FOR FURTHER INFORMATION CONTACT: Steve Yonkers, US–VISIT Privacy Officer, 245 Murray Lane, SW., Washington, DC 20538, by telephone (202) 298–5200 or by facsimile (202) 298–5201.

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) is publishing a revision to existing Privacy Act systems of records known as Enforcement Operational Immigration Records/Automated Biometric Identification System (ENFORCE/IDENT). The notice for these systems of records was last published in the **Federal Register** on March 20, 2006 (71 FR 13987).

ENFORCE is the primary administrative case management system for DHS' Bureau of Immigration and Customs Enforcement (ICE). IDENT is the primary repository of biometric information held by DHS in connection with its several and varied missions and functions, including, but not limited to: The enforcement of civil and criminal laws (including the immigration law); investigations, inquiries, and proceedings there under; and national security and intelligence activities. IDENT is a centralized and dynamic DHS-wide biometric database that also contains limited biographic and encounter history information needed to place the biometric information in proper context. The information is collected by, on behalf of, in support of, or in cooperation with DHS and its components and may contain personally identifiable information collected by other Federal, state, local, tribal, foreign, or international government agencies.

For business purposes ENFORCE and IDENT were operated jointly. Now, as a part of operational and technical restructuring these systems will be operated independently-IDENT under the management of US–VISIT and ENFORCE under the management of ICE. Consequently, the ENFORCE/IDENT system notice is being split into two system notices: one for ENFORCE and one for IDENT. Until a new notice is published by ICE, ENFORCE continues to operate under the system notice published March 20, 2006 (71 FR 13978).

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this system change to the Office of Management and Budget and to Congress.

DHS/2006–0036

SYSTEM NAME:

DHS Automated Biometric Identification System (IDENT).

SYSTEM LOCATION:

Department of Homeland Security (DHS).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this notice consist of:

A. Individuals whose biometrics are collected by, on behalf of, in support of, or in cooperation with DHS concerning operations that implement and/or enforce laws, regulations, treaties, or orders related to the missions of DHS.

B. Individuals whose biometrics are collected by, on behalf of, in support of, or in cooperation with DHS as part of a background check or security screening connection with their hiring, retention, performance of a job function, or the issuance of a license or credential.

C. Individuals whose biometrics are collected by Federal, state, local, tribal, foreign, or international agencies for national security, law enforcement, immigration, intelligence, or other DHS mission-related functions, and who are the subjects of wants, warrants, or lookouts or any other subject of interest.

CATEGORIES OF RECORDS IN THE SYSTEM:

IDENT contains biometric, biographic, and encounter-related data for operation/production, testing, and training environments. Biometric data includes, but is not limited to, fingerprints and photographs. Biographical data includes, but is not limited to, name, date of birth, nationality, and other personal descriptive data. The encounter data provides the context of the interaction with an individual including, but not limited to, location, document numbers, and reason fingerprinted. Test data may be real or simulated biometric, biographic, or encounter related data.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

6 U.S.C. 202, 8 U.S.C. 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1379, and 1732.

PURPOSE(S):

This system of records is established and maintained to enable DHS to carry out its assigned national security, law enforcement, immigration, intelligence and other DHS mission-related functions, and to provide associated testing, training, management reporting, planning and analysis, or other administrative uses by providing a DHS-wide repository of biometrics captured in DHS or law enforcement encounters.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3), limited by privacy impact assessments, data sharing, or other agreements, as follows:

A. To appropriate Federal, state, local, tribal, foreign, or international Governmental agencies seeking information on the subjects of wants, warrants, or lookouts, or any other subject of interest, for purpose related to

administering or enforcing the law, national security, immigration, or intelligence, where consistent with a DHS mission-related function as determined by DHS.

B. To appropriate Federal, state, local, tribal, foreign, or international government agencies charged with national security, law enforcement, immigration, intelligence, or other DHS mission-related functions in connection with the hiring or retention by such an agency of an employee, the issuance of a security clearance, the reporting of an investigation of such an employee, the letting of a contract, or the issuance of a license, grant, loan, or other benefit by the requesting agency.

C. To an actual or potential party or to his or her attorney for the purpose of negotiation or discussion on such matters as settlement of the case or matter, or discovery proceedings.

D. To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.

E. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. Sections 2904 and 2906.

F. To individuals who are obligors or representatives of obligors of bonds posted.

G. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish a DHS mission function related to this system of records.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Information can be stored in case file folders, cabinets, safes, or a variety of electronic or computer databases and storage media.

RETRIEVABILITY:

Records may be retrieved by biometrics or select personal identifiers.

SAFEGUARDS:

The system is protected through multi-layer security mechanisms. The protective strategies are physical, technical, administrative, and environmental in nature, and provide access control to sensitive data, physical access control to DHS facilities, confidentiality of communications, authentication of sending parties, and personnel screening to ensure that all personnel with access to data are screened through background investigations commensurate with the level of access required to perform their duties.

RETENTION AND DISPOSAL:

The following proposal for retention and disposal is pending approval with National Archives and Records Administration (NARA):

Records that are stored in an individual's file will be purged according to the retention and disposition guidelines that relate to the individual's file (DHS/ICE/USCIS001A).

Testing and training data will be purged when the data is no longer required. Electronic records for which the statute of limitations has expired for all criminal violations or that are older than 75 years will be purged. Fingerprint cards, created for the purpose of entering records in the database, will be destroyed after data entry. Work Measurement Reports and Statistical Reports will be maintained within the guidelines set forth in NCI–95–78–5/2 and NCI–85–78–1/2 respectively.

SYSTEM MANAGER(S) AND ADDRESS:

System Manager, IDENT Program Management Office, US–VISIT Program, U.S. Department of Homeland Security, Washington, DC 20528, USA.

NOTIFICATION PROCEDURE:

To determine whether this system contains records relating to you, write to the US–VISIT Privacy Officer, US–VISIT Program, U.S. Department of Homeland Security, 245 Murray Lane, SW., Washington, DC 20528, USA.

RECORD ACCESS PROCEDURES:

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). A determination as to the granting or denial of access shall be made at the time a request is received. Requests for access to records in this system must be in writing, and should be addressed to the US–VISIT Privacy Officer as noted above. Such request may be submitted either by mail or in person. The envelope and letter shall be clearly marked ''Privacy Officer—Redress Request.'' To identify a record, the record subject should provide his or her full name, date and place of birth; if appropriate, the date and place of entry into or departure from the United States; verification of identity by submitting a copy of fingerprints if appropriate (in accordance with 8 CFR 103.21(b) and/or pursuant to 28 U.S.C. 1746, make a dated statement under penalty of perjury as a substitute for notarization), and any other identifying information that may be of assistance in locating the record. The requestor shall also provide a return address for transmitting the records to be released.

CONTESTING RECORD PROCEDURES:

The major part of this system is exempted from this requirement pursuant to 5 U.S.C. 552a(j)(2) and (k)(2). A determination as to the granting or denial of a request shall be made at the time a request is received. An individual desiring to request amendment of records maintained in this system should direct his or her request to the System Manager noted above or the appropriate FOIA/PA Officer. The request should state clearly what information is being contested, the reasons for contesting it, and the proposed amendment to the information.

RECORD SOURCE CATEGORIES:

Basic information contained in this system is supplied by individuals covered by this system, and other Federal, state, local, tribal, or foreign governments; private citizens; and public and private organizations.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

The Secretary of Homeland Security has exempted this system from 5 U.S.C. 552a(c)(3) and (4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5) and (e)(8); (f)(2) through (5); and (g) pursuant to 5 U.S.C. 552a(j)(2). In addition, the Secretary of Homeland Security has exempted portions of this system from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), and (e)(4)(H) pursuant to 5 U.S.C. 552a(k)(2). These exemptions apply only to the extent that records in the system are subject to exemption pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

Dated: July 19, 2006.

Maureen Cooney,

Acting Chief Privacy Officer.

[FR Doc. E6–11995 Filed 7–26–06; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

Publication and Release of the National Response Plan

AGENCY: Department of Homeland Security.

ACTION: Notice.

SUMMARY: This Notice informs the public that the Department of Homeland