[Federal Register Volume 72, Number 107 (Tuesday, June 5, 2007)]
[Notices]
[Pages 31080-31082]
From the Federal Register Online via the Government Printing Office
[www.gpo.gov]
[FR Doc No: 07-2781]

==========

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2007-0027]

Privacy Act; IDENT System of Records

AGENCY: Privacy Office, Office of the Secretary, Department of Homeland Security.

ACTION: Notice of updated Privacy Act 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 (1) to add a category of records that comprises unique personal identifiers that links individuals with their encounters, biometrics, records, and other data elements and (2) to add a new routine use consistent with Office of Management and Budget Memorandum M-07-16, Attachment 2 that permits DHS to be in the best position to respond in a timely and effective manner in the event of a data breach. This republished system of records notice will replace the previously published system of records notice for the Automated Biometric Identification System, Federal Register on July 27, 2006 (71 FR 42651).

DATES: Written comments must be submitted on or before July 5, 2007.

ADDRESSES: You may submit comments, identified by DOCKET NUMBER DHS-2007-0027 by one of the following methods:

Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

Fax: 1-866-466-5370.

Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

FOR FURTHER INFORMATION CONTACT: Claire Miller, US-VISIT Acting Privacy Officer, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Hugo Teufel III, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

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 an existing Privacy Act system of records known as Automated Biometric Identification System (IDENT). The notice for these systems of records was last published in the Federal Register on July 27, 2006 (71 FR 42651).

DHS is republishing IDENT in order (1) to add a category of records that comprises unique personal identifiers that links individuals with their encounters, biometrics, records, and other data elements and (2) to add a new routine use consistent with Office of Management and Budget Memorandum M-07-16, Attachment 2 that permits DHS to be in the best position to respond in a timely and effective

[[Page 31081]]

manner in the event of a data breach. This republished system of records notice will replace the previously published system of records notice for the Automated Biometric Identification System, Federal Register on July 27, 2006 (71 FR 42651).

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 and customs laws), including investigations, inquiries, and proceedings thereunder; 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, and international agencies. As part of an effort to more accurately identify individuals and ensure that all encounters are appropriately linked, IDENT will generate, store, and retrieve data by unique numbers or sequence of numbers and characters. This SORN update adds a category of records to IDENT to include these unique numbers or sequence of numbers and characters, also known as enumerators that link individuals with their encounters, biometrics, records, and other data elements. Additionally, this SORN adds a new routine consistent with Office of Management and Budget Memorandum M-07-16, Attachment 2 that permits DHS to be in the best position to respond in a timely and effective manner in the event of a data breach.

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/US-VISIT-001

System name:

DHS Automated Biometric Identification System (IDENT).

System location:

US-VISIT, Department of Homeland Security (DHS), Washington, DC 20528.

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 mission 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 in 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, unique machine-generated identifiers, 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. Unique machine-generated identifiers are identifiers that link individuals with their encounters, biometrics, records, and other data elements. Test data may be real or simulated biometric, biographic, encounter, or identifiers 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; 19 U.S.C. 1589a.

Purpose(s):

This system of records is established and maintained to provide a DHS-wide repository of biometrics captures in DHS or law enforcement encounters. This will enable DHS to carry out its DHS national security, law enforcement, immigration, intelligence, and other mission-related functions, and to provide associated testing, training, management reporting, planning and analysis, and other administrative uses, by allowing DHS to positively identify an individual whether the name information is the same or different based on biometrics.

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), as follows:

A. To appropriate federal, state, local, tribal, foreign, or international 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 that employee (but only if the System of Records in which the investigatory files are maintained allows such disclosure), 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 individual who are obligors or representatives of obligors of bonds posted.

G. To contractors, grantees, experts, consultants, 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. Such recipients are required to comply with the Privacy Act, 5 U.S.C. 552a, as amended.

H. To the Department of Justice (DOJ) or other Federal agency for purposes of conducting litigation or proceedings

[[Page 31082]]

before any court, adjudicative, or administrative body when (1) DHS; or (2) Any employee of DHS in his/her official capacity; or (3) Any employee of DHS in his/her individual capacity, where DOJ or DHS has agreed to represent the employee; or (4) The United States or any agency thereof is a party to the litigation or proceeding, or has an interest in such litigation or proceeding.

I. To appropriate agencies, entities, and persons when (1) it is suspected or confirmed that the security or confidentiality of information in the system of records has been compromised; (2) DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or ham to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons when reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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, including but not limited to names, identification numbers, date of birth, nationality, document number, and address.

Safeguards:

The system is protected through multi-layer security mechanisms. The protective strategies are physical, technical, administrative, and environmental in nature, and provide access to 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 in DHS/US-VISIT-001, IDENT.

Testing and training data will be purged when the data is no longer required (GRS 20). 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 at the address in the Notification procedure section above. Such request may be submitted either by mail or in person. The envelope and letter shall be clearly marked ``Privacy Officer--Access/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 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 requesting amendment of records maintained in this system should direct his or her request to the System Manager noted above. 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 from 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: May 25, 2007.

Hugo Teufel III,

Chief Privacy Officer.

[FR Doc. 07-2781 Filed 5-31-07; 1:24 pm]

BILLING CODE 4410-10-M