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

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2007–0039]

Privacy Act; Background Check Services 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: Pursuant to Updated Privacy Act of 1974, the Department of Homeland Security, U.S. Citizenship and Immigration Services, is updating the Background Check Service system of records to include a new category of

individuals, which is other individuals over the age of 18 residing in a prospective adoptive parent's household pursuant to 8 CFR 204.3 (herein referred to as ''other individuals''). Additionally, DHS is adding 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 Background Check System, **Federal Register** on December 4, 2006 (71 FR 070413).

DATES: The established system of records will be effective July 5, 2007.

ADDRESSES: You may submit comments, identified by Docket Number DHS–2007–0039 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: For system related questions please contact: Greg Collett, Branch Chief of Application Support for Office of Field Operations, U.S. Citizenship and Immigration Services, Department of Homeland Security, 20 Massachusetts Avenue, NW., Washington, DC 20520. For privacy issues please contract: Hugo Teufel III, Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION: The Department of Homeland Security (DHS), U.S. Citizenship and Immigration Services (USCIS) is congressionally tasked with processing all immigration benefit applications and petitions. In order to assist in this tasks, USCIS established a system of records that consolidates all background check requests and results on immigration benefit applicants/petitioners. This system of records is called the Background Check Service (BCS). At this time, USCIS is updating this system of records notice to add the following category of individuals to the Background Check System: Other individuals over the age of 18 residing in a prospective adoptive parent's household pursuant to 8 CFR 204.3 (herein referred to as ''other individuals''). Additionally, USCIS is adding 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.

USCIS conducts four different background checks on applicants/petitioners applying for USCIS benefits: (1) A Federal Bureau of Investigation (FBI) fingerprint check, (2) a FBI name check, (3) a Customs and Border Protection (CBP) Treasury Enforcement Communication System/Interagency Border Inspection System (TECS/IBIS) name check, and (4) US–VISIT IDENT fingerprint check. BCS will maintain the requests and results of all background check activity for USCIC.

As a centralized repository containing all background check activity, BCS provides the status and results of background checks required for completion of immigration eligibility petitions and application determinations from one web-based system to geographically dispersed field offices. This system supports USCIS's initiatives to reduce immigration benefit/petition case backlog and provide significant efficiencies in vetting and resolving the background checks that are required for USCIS benefits. Prior to BCS, information relating to the US–VISIT IDENT fingerprint checks, FBI fingerprint checks and the FBI name checks were stored in the FD–258 system and FBI Query system respectively. Information relating to the TECS/IBIS name checks was not stored in any system.

The information maintained in BCS is initially collected and maintained in one of the following USCIS case management systems and then it is transferred to BCS:

- Computer-Linked Application Information Management System (CLAIMS) 3, which is used to process applications including, but not limited to, an Adjustment of Status (Green Card) and Temporary Protective Status (TPS);
- CLAIMS 4, which is used to process applications for Naturalization;
- Refugee Asylum Parole System (RAPS), which is used to process Asylum applications; and
- Marriage Fraud Assurance System (MFAS), which is used for processing information relating to investigations of marriage fraud.

The benefit applicant/petitioner and other individuals do not have direct interaction with BCS.

The above systems will send necessary and relevant information to BCS in order to generate a Name Check Request for both the FBI name check and TECS/IBIS name check. Both the requests and results will be stored in BCS.

Applicants and other individuals submit information at the time the fingerprints are taken in order to conduct the FBI fingerprint check and the US–VISIT IDENT fingerprint check. Fingerprints are taken electronically at USCIS Application Support Centers (ASC) or taken from hard copy fingerprint cards (FD–258) that are submitted for those applicants and other individuals who are unable to go to an ASC. The fingerprints are currently stored in the Benefit Biometric Support System (BBSS), which interfaces directly with FBI's Integrated Automated Fingerprint Identification System (IAFIS). The FBI provides responses to the FBI fingerprint check electronically and responses are stored in BCS. US–VISIT IDENT fingerprint check provides responses to BCS.

All information is currently collected as part of the established USCIS application/petition process and is required to verify the applicant/petitioner's eligibility for the benefit being sought. The FBI fingerprint check consists of a search of the FBI's Criminal Master File via IAFIS. This search will identify applicants/petitioners and other individuals who have an arrest record. The FBI Name Check consists of a search of the FBI's Universal Index that includes administrative, applicant, criminal, personnel, and other files compiled for law enforcement purposes. The TECS/IBIS Name Check consists of a search of a multi-agency database containing information from 26 different agencies. The information in TECS/IBIS includes records of known and suspected terrorists, sex offenders, and other individuals that may be of interest to the law enforcement community. USCIS will use TECS/IBIS to access National Crime Information Center (NCIC) records on wanted persons, criminal histories, and previous federal inspections. The information in US–VISIT IDENT links information on individuals with their encounters, biometrics, records, and other data elements.

The information collected in BCS as part of the background check process provides USCIS with information about an applicant/petitioner and other individuals that have national security or public safety implications or indicia of fraud. Collecting this information and taking action to prevent potentially undesirable and often dangerous people from staying in this country clearly supports two primary missions of DHS: Preventing terrorist attacks within the United States and reducing America's vulnerability to terrorism, while facilitating the adjudication of lawful benefit applications.

USCIS will use the results of these background checks to make eligibility determinations, which will result in the approval or denial of a benefit. If fraudulent or criminal activity is detected as a result of the background check, USCIS will forward the information to appropriate law enforcement agencies including Immigration and Customs Enforcement (ICE), FBI, CBP, and/or local law enforcement.

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a ''system of records.'' A ''system of records'' is a group of any records under the control of an agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system to make agency recordkeeping practices transparent, to notify individuals of the uses to which personally identifiable information is put, and to assist the individual in more easily finding such files within the agency.

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

DHS–USCIS–002

SYSTEM NAME:

Background Check Service (BCS). Security Classification: Sensitive but Unclassified.

SYSTEM LOCATION:

The primary BCS system is located at a Department of Homeland Security (DHS) approved data center in the Washington, DC, metropolitan area. Backups are maintained offsite. BCS will be accessible world-wide from all USCIS field offices, service centers, and ASC that are part of the DHS Network.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by this notice consist of:

A. All individuals who are applying for benefits and or who are petitioning on behalf of individuals applying/petitioning for benefits pursuant to the Immigration and Nationality Act of 1952, as amended, 101 [8 U.S.C. 1101] (a)(b).

B. All individuals over the age of 18 residing in a prospective adoptive parent's household whose principal or only residence is the home of the prospective adoptive parents pursuant to 8 CFR 204.3 (herein referred to as ''other individuals'').

CATEGORIES OF RECORDS IN THE SYSTEM:

BCS maintains four general categories of records: Applicant/petitioner identification information, other individual identification information, Background Check Request information, and Background Check Result information.

A. Applicant/Petitioner information includes biographic information associated with each applicant/petitioner including, but not limited to: Name, date of birth, country of birth, address, and employment status. The applicant/petitioner information also includes uniquely identifiable numbers, including but not limited to: Alien number, z-number, receipt number, social security number, armed forces identification number, etc. This information would be derived from newly created benefit applications in USCIS Systems of Records or an update to previously submitted benefit applications.

B. Information related to other individuals over the age of 18 residing in a prospective adoptive parent's household would be derived from newly created inter-country adoption applications pursuant to 8 CFR 204.3. The information collected about these individuals includes: Full name and date of birth.

C. Background Check Request information contains data necessary to perform a background check through the US–VISIT IDENT fingerprint check, FBI fingerprint check, FI name check, and CBP IBIS name check services. This data may include: Transaction control numbers associated with FBI fingerprint checks, receipt numbers, date/time of submission, physical description of subject, and a reason for the submission of the application (i.e. USCIS form code). This category also covers logs associated with the requests of background checks, which may include: Requesting location and requesting person.

D. Background Check Result information encompasses data received from FBI and DHS. This data may include: Identifying transactional information (i.e. transaction control number), biographical information, a subject's FBI information sheet (informally known as a RAP Sheet) as a result of an FBI fingerprint check, an FBI name check report, information from the CBP IBIS database, and information from US–VISIT IDENT fingerprint check. The CBP IBIS database includes data from TECS and NCIC databases.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

8 U.S.C. 1103(a).

PURPOSE(S):

BCS is a single, centralized system that records, reconciles, and stores Background Check Requests and Results of applicants and petitioners seeking USCIS benefits. The following types of background checks will be recorded by BCS: FBI Name Checks, TECS/IBIS Name Checks, and FBI Fingerprint Checks. The collection of information is required to verify the applicant/petitioner's eligibility for USCIS benefits. A background check of varying degree, determined by the benefit/petition, is required for any individual applying for USCIS benefits. In order to seek USCIS benefits, the applicant/petitioner must provide USCIS with all requested information.

In the case of other individuals over the age of 18 residing in a prospective adoptive parent's household, USCIS collects their information to facilitate the appropriate USVISIT IDENT, FBI Name Checks, TECS/IBIS Name Checks, and FBI Fingerprint Checks. This check is conducted in order to assess whether the child will be placed in a safe environment.

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 the United States Department of Justice (DOJ) (including United States Attorney offices) or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: (a) DHS, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent said employee, or (d) the United States or any agency thereof;

B. To another Federal agency (including the Merit Systems Protection

Board and the Equal Employment Opportunity Commission), or to a court, or a party in litigation before a court or in an administrative proceeding being conducted by a Federal agency, when the Government is a party to the judicial or administrative proceeding.

C. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law.

D. To a Congressional office, for 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. 2904 and 2906.

F. 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, in compliance with the Privacy Act of 1974, as amended.

G. To appropriate Federal, state, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, or license, where USCIS believes the information would assist enforcement of civil or criminal laws;

H. To Federal and foreign government intelligence or counterterrorism agencies or components where USCIS becomes aware of an indication of a threat or potential threat to national or international security, or where such use is to assist in anti-terrorism efforts and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure;

I. To a Federal, state, local, tribal, territorial, foreign, or international agency, if necessary to obtain information relevant to a Department of Homeland Security decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit.

J. 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 harm 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:

Records in the system will be stored in a central computer database.

RETRIEVABILITY:

A combination of the following BCS data elements may be used to initiate a query in order to retrieve data from the BCS User Interface. These data elements include, an individual's alien file number, name and date of birth; and receipt number.

SAFEGUARDS:

Information in this system is safeguarded in accordance with applicable laws and policies, including the DHS Information Technology Security Program Handbook. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include restricting access to authorized personnel who have a need-to-know, using locks, and password protection identification features. The system is also protected through a multi-layer security approach. 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 USCIS proposal for retention and disposal is pending approval by the National Archives and Records Administration. Records are stored and retained in the BCS Repository for 75 years, during which time the records will be archived. The 75-year retention rate is based on the length of time USCIS may interact with a customer. For example, background checks are conducted on individuals/petitioners from the age of 14 and up. Retaining the data for this period of time also will enable USCIS to fight identify fraud and misappropriated benefits.

SYSTEM MANAGER(S) AND ADDRESS:

Greg Collett, Branch Chief of Application Support for Office of Field Operations, U.S. Citizenship and Immigration Services, Department of Homeland Security, 20 Massachusetts Avenue, NW., Washington, DC 20529.

NOTIFICATION PROCEDURE:

All individuals applying for immigration benefits are presented on the USCIS form, a Privacy Act Statements and a Signature and Authorization for Release of personally identifiable information. All forms must be signed by the individual. These two notices supply individuals with information regarding uses of the data.

RECORD ACCESS PROCEDURES:

To determine whether this system contains records relating to you, write the USCIS Freedom of Information Act/Privacy Act officer. Mail request to: Elizabeth S. Gaffin, Privacy Officer, Department of Homeland Security, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue, NW., Room 4210, Washington, DC 20529.

CONTESTING RECORD PROCEDURES:

See the ''Notification Procedure'' above.

RECORD SOURCE CATEGORIES:

Information contained in this system of records is obtained from USCIS systems including: CLAIMS3, CLAIMS4, RAPS, and MFAS. Information contained in the system is also obtained from the FBI and DHS. All information contained in BCS is derived from the above systems.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: May 25, 2007.

Hugo Teufel, III,

Chief Privacy Officer.

[FR Doc. 07–2782 Filed 5–31–07; 1:24 pm]

BILLING CODE 4410–10–M