9110-9B P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2017-0039]

Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of a New System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to establish a new DHS system of records titled, "Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records." This system of records allows the DHS to receive, maintain, and disseminate biometric and associated biographic information from non-DHS entities, both foreign and domestic, for the following purposes pursuant to formal or informal information sharing agreements or arrangements ("external information"), or with the express approval of the entity from which the Department received biometric and associated biographic information: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.

Department of Homeland Security/ALL-041 External Biometric Records (EBR) System of Records (SOR) is one of two replacement system of records notices (SORN) for DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT). This SORN applies to records provided to DHS by non-DHS entities that do not fall under existing Component/DHS SORNs. The other replacement for the IDENT SORN will be a

forthcoming technical SORN focused on the technical aspects of the IDENT system. After the technical SORN is published, DHS will rescind the IDENT SORN by publishing a *notice of rescindment* in the *Federal Register*. Components are responsible for maintaining SORN coverage for biometric and associated biographic information collected by that Component.

Additionally, DHS is issuing a Notice of Proposed Rulemaking (NPRM) to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the *Federal Register*. This newly established system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. This new system will be effective upon publication, with the exception of the routine uses, which will become effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number DHS-2017-0039 by one of the following methods:

- Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.
- Fax: 202-343-4010.
- Mail: Philip S. Kaplan, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

Instructions: All submissions received must include the agency name and docket number DHS-2017-0039. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

FOR FURTHER INFORMATION CONTACT: For general questions and for privacy issues, please contact: Philip S. Kaplan, privacy@hq.dhs.gov, (202) 343-1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In 2007, DHS published the IDENT SORN. Since then, the Department's Privacy Act framework and the IDENT information technology system have evolved as the Department has matured. DHS Component SORNs now govern the function and use of the biometrics records collected by each Component. The Department, however, still requires a SORN to cover biometrics received from non-DHS entities. Therefore, DHS is establishing DHS/ALL-041 External Biometric Records (EBR) System of Records, which governs the maintenance and use of biometrics and associated biographic information received from non-DHS entities that are not covered by an existing DHS Component SORNs. A forthcoming technical SORN will cover the limited information created by the IDENT system. Eventually, both this EBR SORN and the planned technical SORN will replace the IDENT SORN. In the meantime, to avoid any gap in SORN coverage for biometrics and associated biographic information, the EBR and

IDENT SORNs will co-exist. After the technical SORN is published, DHS will rescind the IDENT SORN by publishing a *notice of rescindment* in the *Federal Register*.

External information is collected by non-DHS entities, including the Department of Defense (DoD), the Department of Justice (DOJ), State and local law enforcement authorities, or foreign governments. External information shared with DHS includes biometric (e.g., latent fingerprints) and associated biographic information that may be used by DHS for the following purposes: law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities.

DHS also maintains this information to support its information sharing agreements and arrangements with foreign partners to: prevent travelers from assuming different identities to fraudulently gain admission or immigration benefits; identify individuals who seek to enter the United States for unauthorized purposes; identify those who have committed serious crimes or violated immigration law; enable informed decisions on visas, admissibility, or other immigration benefits. Such sharing augments the law enforcement and border control efforts of both the United States and its partners. Additionally, DHS is using this information in concert with external partners to facilitate the screening of refugees in an effort to combat terrorist travel consistent with DHS's and Components' authorities.

Consistent with DHS's mission, information covered by DHS/ALL-041 EBR may be shared with DHS Components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligence, or other homeland

security functions. In addition, DHS may share information with appropriate Federal, State, local, tribal, territorial, foreign, or international government agencies from the providing external entity, consistent with any applicable laws, rules, regulations, and information sharing and access agreements or arrangements. DHS may share biometric and associated biographic information as permitted pursuant to an applicable Privacy Act authorized disclosure, including routine uses set forth in this SORN.

Additionally, DHS is issuing a NPRM to exempt this system of records from certain provisions of the Privacy Act elsewhere in the *Federal Register*. This newly established system will be included in DHS's inventory of record systems.

II. Privacy Act

The Privacy Act embodies fair information practice principles in a statutory framework governing the means by which Federal Government agencies collect, maintain, use, and disseminate individuals' records. 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 an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass U.S. citizens and lawful permanent residents. Additionally, the Judicial Redress Act (JRA) provides a statutory right to covered persons to make requests for access and amendment to covered records, as defined by the JRA, along with judicial review for denials of such requests. In addition, the JRA prohibits disclosures of covered records, except as otherwise permitted by the Privacy Act.

Below is the description of the DHS/ALL-041 External Biometric Records (EBR) System of Records.

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

SYSTEM NAME AND NUMBER: Department of Homeland Security (DHS)/ALL-041 External Biometric Records (EBR) System of Records.

SECURITY CLASSIFICATION: Unclassified, Sensitive. The data may be retained on classified networks but this does not change the nature and character of the data until it is combined with classified information.

SYSTEM LOCATION: Records are maintained at Data Center 1 at Stennis, Mississippi, Data Center 2 at Clarksville, Virginia, at the Office of Biometric Identity Management (OBIM) Headquarters in Washington, D.C., and field offices. The records are maintained in the Information Technology (IT) system, Automated Biometric Identification System (IDENT), also referred to as the Homeland Advanced Recognition Technology (HART).

DHS replicates records from this operational IT system and maintains them in other IT systems connected on the DHS unclassified and classified networks.

SYSTEM MANAGER(S): System Manager, IDENT Program Management Office, OBIM, U.S. Department of Homeland Security, Washington, D.C. 20528; email: OBIMprivacy.ice.dhs.gov.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 6 U.S.C. secs. 202 and 482; 8 U.S.C. secs. 1103, 1105, 1158, 1159, 1187, 1201, 1225, 1254a, 1254b, 1301-1305, 1324, 1357, 1360, 1365a, 1365b, 1372, 1379, 1440f, 1537, 1721, 1722, 1731, and 1732;

14 U.S.C. secs 89, 95; 19 U.S.C. sec. 1589a; 42 U.S.C. sec. 5197a; 44 U.S.C. sec. 3544; 46 U.S.C. sec. 70123; 49 U.S.C. secs. 114, 5103, 40103(b), 40113(a), 44903(b), 44936, 44939, and 46105; 5 CFR part 731; 5 CFR part 732; 32 CFR sec. 147.24; 8 CFR sec. 214.1; 8 CFR sec. 235.1; E.O. 12968 (60 FR 40245), 3 CFR, 1995 Comp. p. 1365.; 13764 (82 FR 8115)., Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors (Aug. 27, 2004); HSPD-11: Comprehensive Terrorist-Related Screening Procedures (Aug. 27, 2004); and National Security Presidential Directive/NSPD-59/HSPD-24: Biometrics for Identification and Screening to Enhance National Security (June 5, 2008).

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to process and maintain biometric and associated biographic information from non-DHS entities, both foreign and domestic, for law enforcement, national security, immigration screening, border enforcement, intelligence, national defense, and background investigations relating to national security positions, credentialing, and certain positions of public trust, consistent with applicable DHS authorities. DHS may use and share these external biometric and associated biographic records for these same purposes, as permitted and approved by our partners, if applicable, pursuant to the agreement or arrangement.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Individuals covered by EBR include the individuals whose biometric and associated biographic information are collected by *non-DHS entities* for the following DHS purposes:

- Background checks and suitability screening;
- National security;

- Law enforcement operations (including individuals who are removed from a foreign country by a foreign partner government based on a criminal conviction);
- Intelligence;
- Border enforcement and immigration screening; and
- National defense.

CATEGORIES OF RECORDS IN THE SYSTEM: Information collected by a *non-DHS entity* and maintained in this system includes:

- Biometric data, including:
    - Facial images;
    - Fingerprints;
    - Latent fingerprints;
    - Iris images;
    - Palm prints;
    - Voice;
    - Scars, marks, and tattoos;
    - DNA or DNA Profile; and
    - Other modalities.

- Biometric-associated biographic data including:
    - Full name (i.e., first, middle, last, nicknames, and aliases);
    - Date of birth (DOB);
    - Gender;
    - Personal physical details, such as height, weight, eye color, and hair color;
    - Signature;
    - Assigned number identifiers, such as, but not limited to, Alien Registration Number (A-Number), Social Security number (SSN), state identification number, civil record number, other agency system specific fingerprint record locator information, Federal Bureau of Investigation (FBI) Number (FNU)/Universal Control Number (UCN), Encounter Identification Number (EID), Finger Identification Number (FIN), DoD Biometric Identifier (DoD BID), Transaction Control Number (TCN), Global Unique Identifier (GUID), National Unique Identification Number (NUIN)), document information and identifiers (e.g., passport and visa data, document type, document number, country of issuance), when available; and

    - Identifiers for citizenship and nationality, including person-centric details, such as country of birth, country of citizenship, and nationality, when available.

- Derogatory information (DI), if applicable, including, wants and warrants, Known or Suspected Terrorist (KST) designation, sexual offender registration, foreign criminal convictions, and immigration violations, when available;
- Miscellaneous officer comment information, when available; and
- Encounter data, including location and circumstance of each instance resulting in biometric collection.

RECORD SOURCE CATEGORIES: EBR SOR receives biometric and associated biographic information from non-DHS entities that may be used by DHS for a wide array of purposes, including those listed in the purpose(s) of the system stated above. EBR maintains records in accordance with the terms of the agreements or arrangements under which partners provide the external information to DHS. Records from external Federal partners include information from the following non-DHS systems of records, last published at:

- JUSTICE/INTERPOL-001 INTERPOL-United States National Central Bureau (USNCB) Records System, 75 FR 27821 (May 18, 2010) [Note: records shared with DHS include: law enforcement, intelligence, and national security records];

- JUSTICE/DOJ-005 Nationwide Joint Automated Booking System, 72 FR 3410 (Jan. 25, 2007), 71 FR 52821 (Sept. 7, 2006);
- JUSTICE/FBI-009 Next Generation Identification (NGI) System of Records (pending DOJ release);
- JUSTICE/FBI-019 Terrorist Screening Records System of Records, 76 FR 77847 (Dec. 14, 2011);
- A0025-2 SAIS DoD Defense Biometric Services, 74 FR 48237 (Sept. 22, 2009);
- A0025-2 PMG (DFBA) DoD Defense Biometric Identification Records System, 80 FR 8292 (Feb. 17, 2015);
- STATE-39 Visa Records 60 FR 39469 (Oct. 25, 2012);
- STATE-36, Security Records 80 FR 77691 (Dec. 15, 2015).

EBR SOR receives biometric and associated biographic information from foreign partners consistent with various international information sharing and access agreements or arrangements on file with DHS Office of Policy, International Affairs.

EBR SOR receives biometric and associated biographic information from State and local partners consistent with various law enforcement information sharing and access agreements or arrangements.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. sec. 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. sec. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation:

1. DHS or any Component thereof;

2. Any employee or former employee of DHS in his/her official capacity;

3. Any employee or former employee of DHS in his/her individual capacity when DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof.

B. 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.

C. To the National Archives and Records Administration (NARA) or General Services Administration pursuant to records management inspections being conducted under the authority of 44 U.S.C. secs. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that there has been a breach of the system of records; (2) DHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals,

DHS (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with DHS's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

F. To another Federal agency or Federal entity, when DHS determines that information from this system of records is reasonably necessary and otherwise compatible with the purpose of collection to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

G. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

H. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory

violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

I. To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS 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 and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

J. To a Federal, State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order (E.O.), or other applicable national security directive.

K. To Federal and foreign government intelligence or counterterrorism agencies or Components when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, or when disclosure supports the conduct of national intelligence and security investigations or assists in anti-terrorism efforts.

L. To a foreign government to notify it concerning its citizens or residents who are incapacitated, unaccompanied minors, or deceased.

M. To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations, with the approval of the Chief Privacy Officer, when DHS identifies a need to use relevant data for purposes of testing new technology.

N. To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information, when disclosure is necessary to preserve confidence in the integrity of DHS, or when disclosure is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent the Chief Privacy Officer determines that release of the specific information in the context of a particular case would constitute a clearly unwarranted invasion of personal privacy.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: DHS stores records in this system electronically in secure facilities protected through multi-layer security mechanisms and strategies that are physical, technical, administrative, and environmental in nature. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by biometrics or select personal identifiers, including but not limited to names, identification numbers, dates of birth, nationality, document number, and address.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Record Schedule DAA-0563-2013-0001 for DHS's biometric and biographic records used for national security, law enforcement, immigration, and other functions consistent with DHS authorities has been approved by National Archives and Records Administration (NARA). EBR records include:

1. Law Enforcement Records: Identification, investigation, apprehension, and/or removal of aliens unlawfully entering or present in the United States and facilitate legal entry of individuals into the United States, which must be destroyed or deleted 75 years after the end of the calendar year in which the data is gathered.
2. Records related to the analysis of relationship patterns among individuals and organizations that are indicative of violations of the customs and immigration laws including possible terrorist threats from non-obvious relationships and specific leads and law enforcement intelligence for active and new investigations. These records must be destroyed or deleted 15 years after the end of calendar year of last use of individual's data.

The latent biometric retention schedule is currently in development with OBIM Headquarters and will be submitted thereafter to NARA for approval.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS safeguards records in this system according to applicable rules and policies, including all applicable DHS automated systems security and access policies. DHS has imposed strict controls to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances or permissions.

RECORD ACCESS PROCEDURES: The Secretary of Homeland Security has exempted this system from the notification, access, and amendment procedures of the Privacy Act, and consequently the Judicial Redress Act if applicable, because it is a law

enforcement system. However, DHS will consider individual requests to determine whether or not information may be released. Thus, individuals seeking access to and notification of any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the Chief Privacy Officer and FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "Contacts Information." If an individual believes more than one Component maintains Privacy Act records concerning him or herself, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, Washington, D.C. 20528-0655. Even if neither the Privacy Act nor the Judicial Redress Act provide a right of access, certain records about the individual may be available under the Freedom of Information Act.

When seeking records about one from this system of records or any other Departmental system of records, the request must conform with the Privacy Act regulations set forth in 6 CFR part 5. The individual must first verify his or her identity, meaning that he or she must provide his or her full name, current address, and date and place of birth. The individual must sign the request, and the signature must either be notarized or submitted under 28 U.S.C. sec. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, an individual may obtain forms for this purpose from the Chief Privacy Officer and Chief Freedom of Information Act Officer, http://www.dhs.gov/foia or 1-866-431-0486. In addition, the individual should:

- Explain why he or she believe the Department would have information being requested;

- Identify which Component(s) of the Department he or she believes may have the information;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the FOIA staff determine which DHS Component agency may have responsive records;

If the request is seeking records pertaining to another living individual, the person seeking the records must include a statement from the subject individual certifying his/her agreement for the requestor to access his or her records.

Without the above information, the Component(s) may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

CONTESTING RECORD PROCEDURES: For records covered by the Privacy Act or covered JRA records, see "Record Access Procedures" above, and 6 CFR Part 5.

NOTIFICATION PROCEDURES: See "Record Access Procedures."

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(j)(2), has exempted this system from the following provisions of the Privacy Act: 5 U.S.C. sec. 552a(c)(3), (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(5), and (e)(8); (f); and (g)(1) through (5). Additionally, the Secretary of Homeland Security, pursuant to 5 U.S.C. sec. 552a(k)(2) and (k)(5), has exempted this system from the following provisions of the Privacy Act, 5 U.S.C. sec. 552a(c)(3); (d); (e)(1), (e)(4)(G), (e)(4)(H); and (f).

Exemptions from these particular subsections are justified on a case-by-case basis determined at the time a request is made. When this system receives a record from another system exempted in that source system under 5 U.S.C. 552a(j)(2), DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated and claim any additional exemptions set forth here.

HISTORY: Records in this System of Records were previously covered under DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007).

Philip S. Kaplan,
Chief Privacy Officer,
Department of Homeland Security.
[FR Doc. 2018-08453 Filed: 4/23/2018 8:45 am; Publication Date: 4/24/2018]