<NOTICE>

<PREAMB>

<AGENCY TYPE='S'>DEPARTMENT OF HOMELAND SECURITY

<DEPDOC>[Docket No. DHS-2019-0047]

<SUBJECT>Privacy Act of 1974; System of Records

AGENCY: Department of Homeland Security.

ACTION: Notice of 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-043 Enterprise Biometric Administrative Records (EBAR) System of Records (SOR)." This system of records allows the DHS to collect and maintain administrative and technical records associated with the enterprise biometric system known as the Automated Biometric Identification System (IDENT) and its successor information technology system, currently in development, called the Homeland Advanced Recognition Technology (HART).

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 **April 10, 2020**. This new system will be effective upon publication, with the exception of the routine uses, which will become effective **April 10, 2020**.

ADDRESSES: You may submit comments, identified by docket number DHS-2019-0047 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: Jonathan R. Cantor, Acting 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-2019-0047. 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: Jonathan R. Cantor, privacy@hq.dhs.gov, (202) 343-1717, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In 2007, DHS published the DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT), 72 FR 31080 (June 5, 2007) system of records notice (SORN). The IDENT SORN covered biometric holdings for the entire Department. Since then, the Department's Privacy Act framework and technology for enterprise biometrics has evolved as the Department has matured. DHS Component SORNs now cover the

collection, maintenance, and use of the biometrics records collected directly by each Component. The Department, however, still published a SORN to cover biometrics first collected and received from non-DHS entities, DHS/ALL-041 External Biometric Records (EBR) SORN, 83 FR 17829 (April 24, 2018), which governs the maintenance and use of biometrics and associated biographic information received from non-DHS entities. DHS is establishing DHS/ALL-043 Enterprise Biometric Administrative Records (EBAR) to cover the administrative and technical records associated with the enterprise biometric system, known as the Automated Biometric Identification System (IDENT) and its successor information technology system, currently in development, called the Homeland Advanced Recognition Technology (HART). Together, the EBAR SORN, EBR SORN, and the underlying Component SORNs will replace the IDENT and Technical Reconciliation Analysis Classification System (TRACS) SORNs. DHS will rescind the IDENT and TRACS SORNs by publishing a *notice of rescindment* in the *Federal Register*, following publication of this SORN.

The Office of Biometric Identity Management (OBIM) maintains the Department's primary repository of biometric information held by DHS in connection with varied missions and functions, including law enforcement; national security; immigration screening; border enforcement; intelligence; national defense; background investigations relating to national security positions; and credentialing consistent with applicable DHS authorities.

The primary repository, currently IDENT and its successor information technology (IT) system, HART, 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 Federal, state, local, tribal, foreign, or international agencies, consistent with any applicable laws, rules, regulations, and information sharing and access agreements or arrangements.

Component system SORNs and the DHS/ALL-041 EBR SORN cover the biometric data itself, but OBIM's biometric repository generates technical and administrative information necessary to carry out functions that are not explicitly outlined in component source-system SORNs. For example, to more accurately identify individuals and ensure that all encounters are appropriately linked, IDENT and its successor IT system, HART, will generate, store, and retrieve data by unique numbers or sequence of numbers and characters. These unique numbers or sequence of numbers and characters, also known as enumerators, link individuals with their encounters, biometrics, records, and other data elements. The EBAR SOR will be used for OBIM analysis and reporting functions in support of international data sharing efforts, redress functions, and the reporting and analysis functions of OBIM.

Consistent with DHS's mission, information covered by DHS/ALL-043 EBAR 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 consistent with the routine uses set forth in this system of records notice.

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 covered persons with a statutory right 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-043 Enterprise Biometrics Administrative Records (EBAR) 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.

<SIG><PRIACT><HD2>SYSTEM NAME AND NUMBER:

Department of Homeland Security (DHS)/ALL-043 Enterprise Biometric Administrative Records (EBAR) System of Records.

<HD2>SECURITY CLASSIFICATION:

Unclassified. 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.

<HD2>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), and the successor Homeland Advanced Recognition Technology (HART). HART records will be maintained in the FedRAMP-approved Amazon Web Services U.S. cloud environment.

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

<HD2>SYSTEM MANAGER(S):

System Manager, IDENT/HART Program Management Office, OBIM, U.S. Department of Homeland Security, Washington D.C. 20528; email OBIMprivacy@ice.dhs.gov.

<HD2>AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

6 U.S.C. secs. 202 and 482; 8 U.S.C. secs., 1365a, 1365b, 1379, 1722, 1731, and 1732; 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).

<HD2>PURPOSE(S) OF THE SYSTEM:

This system will enable execution of administrative functions of the biometric repository such as redress operations, testing, training, data quality and integrity, utility, management reporting, planning and analysis, and other administrative uses.

<HD2>CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals covered by EBAR include the individuals whose biometric and associated biographic information are collected by both DHS and non-DHS entities.

<HD2>CATEGORIES OF RECORDS IN THE SYSTEM:

The unique records generated by EBAR include unique machine-generated identifiers (e.g., Encounter Identification Number (EID), fingerprint identification number (FIN), and Transaction Control Number (TCN)) that link individuals with their encounters, biometrics, records, and other data elements.

<HD2>RECORD SOURCE CATEGORIES:

The categories of records covered by the EBAR SOR are derived and created from biometric and associated biographic information received by DHS from non-DHS entities covered by the DHS/ALL-041 Enterprise Biometric Records System of Records, and DHS entities (e.g., U.S. Customs and Border Protection, U.S. Citizenship and Immigration Services, Federal Emergency Management Agency, Transportation Security Administration, U.S. Immigration and Customs Enforcement, U.S. Coast Guard) which are the original collectors of the biometrics and covered by their own system SORNs:

- DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088, (Feb. 23, 2010);

- DHS/ALL-026 Department of Homeland Security Personal Identity Verification Management System, 74 FR 30301 (June 25, 2009);
- DHS/CBP-002 Global Enrollment System, 78 FR 3441 (Jan. 16, 2013);
- DHS/CBP-006 Automated Targeting System, 77 FR 30297 (May 22, 2012);
- DHS/CBP-007 Border Crossing Information (BCI), 81 FR 89957 (Dec. 13, 2016);
- DHS/CBP-010 Persons Engaged in International Trade in Customs and Border Protection Licensed/Regulated Activities, 73 FR 77753 (Dec. 19, 2008);
- DHS/CBP-011 U.S. Customs and Border Protection TECS, 73 FR 77778 (Dec. 19, 2008);
- DHS/CBP-021 Arrival and Departure Information System (ADIS), 80 FR 72081 (Nov. 18, 2015);
- DHS/CBP-023 Border Patrol Enforcement Records System of Records (BPER), 81 FR 72601 (Oct. 20, 2016);
- DHS/ICE-006 Intelligence Records System (IIRS), 75 FR 9233 (March 1, 2010);
- DHS/ICE-007 Criminal History and Immigration Verification (CHIVe) System of Records, 83 FR 20844 (May 8, 2018);
- DHS/ICE-009 External Investigations, 75 FR 404 (Jan. 5, 2010);
- DHS/ICE-010 Confidential and Other Sources of Information, 78 FR 7798 (Feb. 4, 2013);
- DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records, 81 FR 72080 (October 19, 2016);
- DHS/ICE-014 Homeland Security Investigations Forensic Laboratory, 81 FR 45523 (July 14, 2016);

- DHS/TSA-001 Transportation Security Enforcement Record System, 83 FR 43888 (Aug. 28, 2018);
- DHS/TSA-021 TSA Pre✓™ Applications Program, 78 FR 55274 (Sept. 10, 2013);
- DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records, 82 FR 43556 (Sept. 18, 2017);
- DHS/USCIS-007 Benefits Information System, 81 FR 72069 (Oct. 19, 2016);
- DHS/USCIS-018 Immigration Biometric and Background Check, 83 FR 36950 (July 31, 2018);
- DHS/USCG-031 USCG Law Enforcement (ULE) System of Records, 81 FR 88697 (Dec. 8, 2016).

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, 82 FR 24151 (May 25, 2017);
- 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-26 Passport Records, 76 FR 34966 (July 6, 2011);
- STATE-36 Security Records, 83 FR 28058 (Jun. 15, 2018);
- STATE-39 Visa Records, 83 FR 28062 (Jun 15, 2018).

<HD2>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 the U.S. Attorneys Offices, or other federal agencies conducting litigation or 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, only 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 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 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.

H. 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.

I. 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.

J. To a Federal, state, tribal, local, international, or foreign government agency or entity in order to provide relevant information related to intelligence, counterintelligence, or counterterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

K. 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.

<HD2>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.

<HD2>POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be retrieved by select personal identifiers; primarily the FIN. The system also allows for queries based on other information in the system including but not limited to unique identification numbers.

<HD2>POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The transactional record systems retention schedule is currently in development with OBIM and will be submitted thereafter to NARA for approval.

<HD2>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.

<HD2>RECORD ACCESS PROCEDURES:

DHS will consider individual requests to determine whether or not information may be released. 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 "FOIA Contact Information." If an individual believes more than one component maintains Privacy Act records concerning him or her, 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 maybe available under the Freedom of Information Act.

When seeking records 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.

<HD2>CONTESTING RECORD PROCEDURES:

For records covered by the Privacy Act or covered JRA records, see "Records Access Procedures" above, and 6 CFR part 5.

<HD2>NOTIFICATION PROCEDURES:

See "Record Access Procedures."

<HD2>EXEMPTIONS PROMULGATED FOR THE SYSTEM:

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

<HD2>HISTORY:

Records in this System of Records were previously covered under DHS/US-VISIT-001 DHS Automated Biometric Identification System (IDENT), 72 Fed. Reg. 31080 (June 5, 2007) and DHS/NPPD/USVISIT-003 Technical Reconciliation Analysis Classification System (TRACS), 73 Fed. Reg. 116 (June 16, 2008).</PRIACT>

<SIG><NAME>Jonathan R. Cantor,
<TITLE>Acting Chief Privacy Officer,
Department of Homeland Security.</SIG>

<FRDOC> [FR Doc. 2020–04979 Filed 3–10–20; 8:45 am]
<BILCOD> BILLING CODE 9110–9B–P
[FR Doc. 2020-04979 Filed: 3/13/2020 8:45 am; Publication Date: 3/16/2020]