DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2019-0004]

Privacy Act of 1974; System of Records

AGENCY: U.S. Citizenship and Immigration Services, Department of Homeland Security.

ACTION: Notice of a Modified System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security (DHS) proposes to modify and reissue a current DHS system of records titled, "Department of Homeland Security/U.S. Citizenship and Immigration Services-011 E-Verify Program System of Records." This system of records describes DHS/U.S. Citizenship and Immigration Services (USCIS) collection and maintenance of records on employers, entities authorized by federal law to use E-Verify, employees in the United States, and individuals subject to employment eligibility verification under E-Verify and E-Verify Self-Check.

DHS/USCIS is updating this system of records notice to: (1) add the Data Universal Numbering System (DUNS) number; (2) add Validation Instrument for Business Enterprises (VIBE) as a new record source; (3) specify under categories of records that information from State Motor Vehicle Agencies can be derived from commercial data providers; (4) update Routine Use E and add Routine Use F to comply with requirements set forth by OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," (Jan. 3, 2017); (5) amend Routine Use J to include disclosure to the National Law Enforcement

Telecommunications System (NLETS)[1] for the purpose of validating information from a driver's license, permit, or identification card issued by a State Motor Vehicle Agency; (6) add Routine Use L for disclosure to persons and other entities authorized by federal law to confirm the employment eligibility of individuals subject to verification under E-Verify; (7) add Routine Use M for disclosure to federal government intelligence or counterterrorism agencies or components when DHS becomes aware of a violation or potential violation of E-Verify program requirements that is related to an indication of a threat or potential threat to national security to assist in countering such a threat; and (8) explain that this system of records covers records from other DHS systems of records that may claim exemptions and DHS will comply with the record source system exemptions when relevant. All following routine uses are being renumbered to account for the additional routine uses. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice. This modified system will be included in DHS's inventory of record systems.

DATES: Submit comments on or before **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. This modified system will be effective upon publication. New or modified routine uses are effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number DHS-2019-0004 by one of the following methods:

[1] NLETS, which is owned by the States, is a 501(c)(3) nonprofit organization that was created over 50 years ago by the principal law enforcement agencies of the States.

- 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-2019-0004. 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, please contact: Donald K. Hawkins, (202) 272-8030, USCIS.PrivacyCompliance@uscis.dhs.gov, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue NW, Washington, D.C. 20529. For privacy questions, please contact: Jonathan R. Cantor, (202) 343-1717, Privacy@hq.dhs.gov, Acting Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528-0655.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, DHS/USCIS proposes to modify and reissue a current DHS system of records titled, "DHS/USCIS-011 E-Verify Program System of Records."

USCIS is modifying this system of records notice (SORN) to (1) add the DUNS number as a category of record; (2) add VIBE as a new record source; (3) specify under

categories of records that information from State Motor Vehicle Agencies can be derived from commercial data providers; (4) update Routine Use E and add Routine Use F to comply with requirements set forth by OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," (Jan. 3, 2017); (5) amend Routine Use J to include disclosure to NLETS for the purpose of validating information from a driver's license, permit, or identification card issued by a state Motor Vehicle Agency; (6) add Routine Use L for disclosure to persons and other entities authorized by federal law to confirm the employment eligibility of individuals subject to verification under E-Verify; (7) add Routine Use M for disclosure to federal government intelligence or counterterrorism agencies or components when DHS becomes aware of a violation or potential violation of E-Verify program requirements that is related to an indication of a threat or potential threat to national security for the purpose of countering such threat; and (8) explain that this system of records covers records from other DHS systems of records that may claim exemptions and DHS will comply with the record source system exemptions when relevant. All following routine uses are being renumbered to account for the additional routine uses. Additionally, this notice includes non-substantive changes to simplify the formatting and text of the previously published notice.

E-Verify is an Internet-based system that allows enrolled participants to electronically confirm the employment eligibility of employees to work in the United States. Participants collect information from the Form I-9, *Employment Eligibility Verification*, completed by the employee, to query against existing information accessed by the Verification Information System (VIS). VIS provides employment authorization

information to employers, entities authorized by federal law to use E-Verify, and to individuals seeking to check employment eligibility under the Immigration and Nationality Act (INA). It may be used by DHS to support DHS monitoring and compliance activities aimed to prevent the commission of fraud, discrimination, or other misuse or abuse of E-Verify, or other violation of law related to employment eligibility verification. E-Verify, in particular, monitors against violations of privacy laws or other illegal activity related to misuse of E-Verify, including for example: (1) investigating duplicate or incomplete enrollments by employers; (2) inappropriate enrollments by individuals posing as employers; (3) verifications that are not performed within the required time limits; and (4) cases referred by and between E-Verify and the Department of Justice Immigrant and Employee Rights Section (formerly known as the Office of Special Counsel for Immigration-Related Unfair Employment Practices), or other intelligence or law enforcement entities.

Additionally, the information in E-Verify may be used for program management and analysis, program outreach, customer service, and preventing or deterring further use of stolen identities in E-Verify.

USCIS also provides services to employees, job seekers, and employers through a free Web-based service: myE-Verify, which provides the following resources:

- Resource Center: Information and learning materials from the employee's perspective about the E-Verify and employment eligibility verification processes, including employee's rights and roles, privacy, as well as the employer's responsibilities.

- Case Tracker: Track the status of the employee's E-Verify case-in-progress and

advises whether any action is required.

- myE-Verify personal accounts: Allows employees to establish a secure personal account to access additional myE-Verify features. Account holders have access to the following features:

    - Self Lock: Protects the employee's identity by preventing unauthorized use of his or her Social Security number (SSN) in E-Verify. Self Lock allows the employee to place a "lock" on his or her SSN. This helps prevent anyone else from using the employee's SSN to try to get a job with an E-Verify employer. The Self Lock feature is only available to myE-Verify account holders.

    - Document Expiration Reminders: When an employee presents a work authorization document with an expiration date, E-Verify will remind the employer when the document is about to expire. This case alert provides a countdown of expiring work authorization documents beginning 90 days before expiration and will show the document as expired for 30 days past expiration.

    - Case History: Allows employees to see where and when their information has been used in E-Verify and Self Check. The Case History feature is only available to myE-Verify account holders.

    - Self Check: Provides individuals the ability to confirm their employment eligibility. Self Check also provides a service that permits individuals who

successfully complete a Self Check case to establish a myE-Verify account. The information collected to register and maintain a myE-Verify account, including information collected for e-authentication purposes, is covered by DHS/ALL-037 E-Authentication System of Records, previously published in the Federal Register at 79 FR 46857 (August 11, 2014).

Consistent with DHS's information sharing mission, records covered by this SORN may be shared with other 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/USCIS 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. USCIS reviews disclosures from this System of Records for compliance with Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA) section 404(h).

This modified 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/USCIS-011 E-Verify Program 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)/U.S. Citizenship Immigration Service (USCIS)-011 E-Verify Program.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at USCIS Headquarters in Washington, D.C. and at DHS/USCIS field offices. Electronic records are stored in the Verification Information System (VIS).

SYSTEM MANAGER(S): Chief, Verification Division, E-Verify@dhs.gov, U.S. Citizenship and Immigration Services, Department of Homeland Security, 131 M Street, N.E., Suite 200, Mail Stop 200, Washington, D.C. 20529.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Public Law 104-208, secs. 401-405 (Sept. 30, 1996), codified at 8 U.S.C. 1324a note.

PURPOSE(S) OF THE SYSTEM: The purpose of this system is to provide employment authorization information to employers, entities authorized by federal law to participate in E-Verify, and to individuals seeking to check employment eligibility under the Immigration and Nationality Act (INA). This system also enables individuals to access features concerning the use of their personally identifiable information (PII) in E-Verify, such as the ability to lock their Social Security number (SSN) to prevent its use in E-Verify and Self Check. The system may also be used by DHS to support DHS monitoring and compliance activities for obtaining information in order to prevent the commission of fraud, discrimination, or other misuse or abuse of the E-Verify system, including violations of privacy laws or other illegal activity related to misuse of E-Verify, including for example: (1) investigating duplicate or incomplete enrollments by employers; (2) inappropriate enrollments by individuals posing as employers; (3) verifications that are not performed within the required time limits; and (4) cases referred by and between E-Verify and the Department of Justice Immigrant and Employee Rights Section (formerly known as the Office of Special Counsel for Immigration-Related Unfair Employment Practices), or other intelligence or law enforcement entities.

Additionally, the information in E-Verify may be used for program management and analysis, program outreach, customer service, and preventing or deterring further use of stolen identities in E-Verify.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Categories of individuals covered by E-Verify, to the extent these individuals are covered by and defined by the Privacy Act and this SORN, include: employees whose employers have submitted identity and employment eligibility information on their behalf; employers or

employer agents that enroll in E-Verify; clients of employer agents who enroll in E-Verify; individuals employed or retained by employers or employer agents who have accounts to use E-Verify; individuals subject to verification by E-Verify; entities authorized by federal law to use E-Verify; entities who contact E-Verify for information on the use of E-Verify; entities who provide their names and contact information to E-Verify for notification or contact purposes; individuals seeking to confirm employment eligibility under the INA using Self Check; and individuals who have created a myE-Verify account.

CATEGORIES OF RECORDS IN THE SYSTEM: Information collected about individuals may include the following:

A. Information about the employee or individual to be confirmed:

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- SSN;
- Home address (address, apartment number, city, state/region);
- Email address;
- Telephone number (home, mobile, work, other);
- Employee's First Day of Employment;
- Claimed citizenship status;

- Form I-9 document type provided by individual to the entity verifying employment eligibility (such as passport, employment authorization document, or permanent resident card);
- Expiration date of acceptable Form I-9 document;
- State or jurisdiction of issuance of identity document when that document is a driver's license, driver's permit, or state-issued identification (ID) card;
- Passport number and country of issuance;
- Driver's license number, driver's permit number, or state-issued ID number;
- Receipt number;
- Visa number;
- Alien Number (A-Number);
- I-94 Number;
- Form I-766, *Employment Authorization Document*, Number; and
- Form I-551, *Permanent Resident Card*, Number and photographs.

B. Disposition data from the employer or entity. If the E-Verify case result is Employment Authorized, E-Verify automatically closes the case and no additional information is collected from the employer or entity. The following codes are entered by the employer or entity when the case result is Final Nonconfirmation (FNC), based on what the employer or entity does as a result of the employment verification query (the most up-to-date disposition codes can be found in the E-Verify User Manual available at https://www.E-Verify.gov):

- [Employer Name] will no longer employ [Employee Name].
- [Employer Name] will continue to employ [Employee Name].

    - If the employer selects the option that he or she will continue to employ the individual, he or she has to provide the reason why he or she will do so in a free text field.
- Neither of the options above apply – I am closing this case for a different reason.
    - If the employer selects the option that he or she is closing the case for another reason, the employer has to select a reason from the following predetermined reasons:
        - SSA (Social Security Administration) asked me to re-run this case
        - DHS (Department of Homeland Security) asked me to re-run this case
        - The information entered was not correct.
        - Other
            - If the employer selects "Other," the employer must type the reason in a free text field.
- Information related to the expiration of the three day hire rule;
    - Whether an individual is awaiting a SSN;
    - Technical problems;
    - Audit revealed new hire was not run;
    - Federal contractor with E-Verify clause verifying existing employees; and
    - Other.

C. Information about the Enrollee, Employer, Entity, or Employer Agent:

- Company name;
- "Doing business as" name (optional);

- Data Universal Numbering System (DUNS) number (only required for employers with Federal Acquisition Regulation (FAR) clause);
- Street address;
- Employer Identification Number (EIN);
- North American Industry Classification System (NAICS) code;
- Number of employees;
- Number of sites;
- Parent company or corporate company;
- Name of company point of contact;
- Phone number;
- Fax number; and
- Email address.

D. Information about the Individual User of E-Verify (e.g., Human Resource employee conducting E-Verify queries):

- Full name (first, middle initial, and last);
- Telephone number (home, mobile, work, other);
- Fax number;
- Email address; and
- User ID.

E. Employment Eligibility Information created by E-Verify:

- Case Verification Number; and

- Verification Information System response (the most up-to-date codes can be found in the E-Verify User Manual available at https://www.E-Verify.gov), for example:
    - Employment authorized;
    - DHS verification in process;
    - SSA Tentative Nonconfirmation (TNC);
    - DHS TNC;
    - Employee referred to SSA;
    - Employee referred to DHS;
    - Close Case and Resubmit;
    - SSA Case in Continuance (In rare cases, SSA needs more than 10 Federal Government workdays to confirm employment eligibility); and
    - DHS Case in Continuance (In rare cases, DHS needs more than 10 Federal Government workdays to confirm employment eligibility);
    - FNC.

F. Information from the National Law Enforcement Telecommunications System (NLETS) and State Motor Vehicle Agencies (MVA) used to verify the information from a driver's license, permit, or state issued ID card. The categories of records from MVAs and MVA information via commercial data providers include:

- Full name (first, middle and last);
- State or Jurisdiction of Issuance;
- Document type (i.e., driver's license, driver's permit, or state-issued ID card);
- Document number;

- Date of birth;
- Status text (e.g., status of the license – valid, revoked, or expired);
- Status description text (i.e., document issue date and/or record found indicator); and
- Expiration date.

G. Information from federal databases used to confirm employment eligibility may contain some or all of the following information about the individual being verified:

- Full name (first, middle, and last);
- Other names or aliases, if available;
- Date of birth;
- Age;
- Country of birth;
- Country of citizenship;
- A-Number;
- SSN;
- Citizenship number;
- Receipt number;
- Home address (address, apartment number, city, state/region);
- Previous Address;
- Phone number;
- Nationality;
- Gender;

- Photograph;
- Date entered into United States;
- Class of admission;
- File Control Office Code;
- Student and Exchange Visitor Information System (SEVIS) Number;
- Form I-94 Number;
- Provision of Law cited for employment authorization;
- Office Code where the authorization was granted;
- Date employment authorization decision was issued;
- Date employment authorization begins;
- Date employment authorization expires;
- Date employment authorization was denied;
- Confirmation of employment eligibility;
- TNC of employment eligibility and justification;
- FNC of employment eligibility;
- Status of Department of Justice Executive Office Immigration Review System (EOIR) information, if in proceedings;
- Date alien's status changed;
- Class of Admission Code;
- Date employee is admitted into the U.S. until;
- Port of Entry;
- Departure date;

- Visa Number;
- Passport Number;
- Passport Country of Issuance (COI);
- Passport Card Number;
- Benefit granting document number, for example, Form I-551, *Permanent Resident Card*, or Form I-766, *Employment Authorization Document*;
- Expiration date;
- Employment Authorization Card information;
- Permanent Resident Card information;
- Employer Identification Number;
- Valid to date;
- Student status;
- Visa Code;
- Status Code;
- Status change date;
- Port of Entry Code;
- Non-Citizen entry date;
- Program end date;
- Naturalization Certificate Number;
- Naturalization date and place;
- Naturalization information and certificate;
- Naturalization verification (Citizenship Certificate Identification ID);

- Naturalization verification (Citizenship naturalization date/time);
- Immigration status (Immigration Status Code);
- Universal Control Number (formerly known as Federal Bureau of Investigation Number);
- Admission Number;
- Date of admission;
- Marital status;
- Marriage date and place;
- Marriage information and Certificate;
- Visa Control Number;
- Visa Foil Number;
- Case history;
- Alerts;
- Case summary comments;
- Case category;
- Date of encounter;
- Encounter information;
- Case actions and decisions;
- Bonds;
- Current status;
- Asylum Applicant Receipt date;
- Airline and Flight Number;

- Country of residence;
- City where boarded;
- City where visa was issued;
- Date visa issued;
- Address while in United States;
- File Number; and
- File location.

H. Information from individuals who successfully complete an E-Verify query using Self Check:

- Full name (first, middle initial, and last);
- Other names or aliases, if available;
- Date of birth;
- SSN; and
- Document(s) type, associated number, and associated expiration date that demonstrates work authorization. These may include U.S. Passport, Form I-766, *Employment Authorization Document*, Form I-551, *Permanent Resident Card*, or other documents and associated numbers listed as acceptable Form I-9, Form I-9 and supporting documents; and Employment Eligibility Verification documents.

I. Information from individuals that establish a lock on their SSN through myE-Verify accounts:

- Full name (first, middle initial, and last);
- Other names or aliases, if available;

- SSN;
- Date of birth;
- Lock Receipt Number;
- Lock date and expiration date;
- Email address; and
- Self-Generated security questions and answers.

RECORD SOURCE CATEGORIES: Records are obtained from several sources including: (A) Information collected from employers and entities about their employees; (B) Information collected from individuals relating to employment eligibility verification; (C) Information collected from E-Verify users used to provide account access and monitoring; (D) Information collected from entities requesting information about E-Verify; (E) Information created by E-Verify; (F) Information from individuals seeking to check employment eligibility and access to features concerning the use of their information in E-Verify and Self Check; (G) Federal and state databases listed below, including the systems and the SORNs that cover information contained in those systems:

- SSA Numident System covered by SSA's Master Files of SSN Holders and SSN Applications SORN, 79 FR 8780 (February 13, 2014), 78 FR 40542 (July 5, 2013), and 75 FR 82121 (December 29, 2010);
- U.S. Customs and Border Protection (CBP) information covered by DHS/CBP-005 Advance Passenger Information System SORN, 80 FR 13407 (March 13, 2015); DHS/CBP-007 CBP Border Crossing Information SORN, 81 FR 89957 (December 13, 2016); DHS/CBP-011 U.S. Customs and Border Protection TECS SORN, 73 FR 77778 (December 19, 2008); DHS/CBP-016 Non-Immigrant

System SORN, 80 FR 13398 (March 13, 2015); DHS/CBP-021 Arrival and Departure Information System SORN, 80 FR 72081 (November 18, 2015); DHS/USVISIT-004 DHS Automated Biometric Identification System (IDENT) SORN, 72 FR 31080 (June 5, 2007); DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN, 82 FR 43556 (September 18, 2017); and DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) SORN, 75 FR 412 (January 5, 2010);

- CBP Nonimmigrant Information System (NIIS) covered by DHS/CBP-016 Non-Immigrant System SORN, 80 FR 13398 (March 13, 2015);
- CBP Border Crossing Information (BCI) covered by DHS/CBP-007 CBP Border Crossing Information SORN, 81 FR 89957 (December 13, 2016);
- U.S. Immigration Customs and Enforcement (ICE) SEVIS covered by DHS/ICE-001 Student and Exchange Visitor Information System (SEVIS) SORN, 75 FR 412 (January 5, 2010); DHS/ALL-016 Correspondence Records SORN, 83 FR 48645 (September 26, 2018); and DHS/ALL-003 Department of Homeland Security General Training Records SORN, 73 FR 71656 (November 25, 2008);
- ICE ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM) Alien Number covered by DHS/ICE-011 Criminal Arrest Records and Immigration Enforcement Records (CARIER) System of Records SORN, 81 FR 72080 (October 19, 2016);
- USCIS Aliens Change of Address System (AR-11) covered by DHS/USCIS-007 Benefit Information System SORN, 81 FR 72069 (October 19, 2016);

- USCIS Central Index System (CIS) covered by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN, 82 FR 43556 (September 18, 2017);
- USCIS Customer Profile Management System (CPMS) covered by DHS/USCIS-018 Immigration Biometric and Background Check (IBBC) System of Records SORN, 83 FR 36950 (July 31, 2018);
- USCIS Computer-Linked Application Information Management System 3 (CLAIMS 3) covered by DHS/USCIS-007 Benefit Information System SORN, 81 FR 72069 (October 19, 2016);
- USCIS Computer-Linked Application Information Management System 4 (CLAIMS 4) covered by DHS/USCIS-007 Benefit Information System SORN, 81 FR 72069 (October 19, 2016);
- USCIS Citizenship and Immigration Services Centralized Operational Repository (eCISCOR);[2]
- USCIS RAILS (a modernization of the National File Tracking System) covered by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN, 82 FR 43556 (September 18, 2017);
- USCIS Microfilm Digitization Application System (MiDAS) covered by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN, 82 FR 43556 (September 18, 2017);

[2] SORN coverage is dependent upon connected IT systems. See Appendix to DHS/USCIS/PIA-023(b) Enterprise Citizenship and Immigrations Services Centralized Operational Repository.

- USCIS Marriage Fraud Amendment System (MFAS) covered by DHS/USCIS-007 Benefit Information System SORN, 81 FR 72069 (October 19, 2016);
- USCIS Enterprise Document Management System (EDMS) covered by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN, 82 FR 43556 (September 18, 2017);
- USCIS Global (formerly known as Refugees, Asylum, and Parole System (RAPS)) covered by DHS/USCIS-010 Asylum Information and Pre-Screening System of Records SORN, 80 FR 74781 (November 30, 2015);
- USCIS Validation Instrument for Business Enterprises (VIBE) covered by DHS/USCIS/ICE/CBP-001 Alien File, Index, and National File Tracking System of Records SORN, 82 FR 43556 (September 18, 2017); DHS/USCIS-006 Fraud Detection and National Security Records (FDNS) SORN, 77 FR 47411 (August 8, 2012); and DHS/USCIS-007 Benefit Information System SORN, 81 FR 72069 (October 19, 2016);
- Department of State Consular Consolidated Database (CCD) covered by STATE-05 Overseas Citizens Services Records and Other Overseas Records, 81 FR 62235, (September 8, 2016); STATE-26 Passport Records, 80 FR 15653 (March 24, 2015); and STATE-39 Visa Records, 83 FR 28062 (June 15, 2018);
- DOJ's Immigration Review Information Exchange System (IRIES) covered by EOIR-001 Records and Management Information System, 69 FR 26179 (May 11, 2004), including routine use updates in 82 FR 24147 (May 25, 2017); and
- State Motor Vehicle Agencies (through commercial data providers).

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 listed below. USCIS reviews disclosures from this System of Records for compliance with IIRIRA section 404(h).

A. To the Department of Justice (DOJ), including Offices of the U.S. Attorneys, or other federal agencies 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 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 employers participating in E-Verify in order to confirm the identity and employment eligibility of their employees working in the United States.

J. To NLETS and the American Association of MVA Network and participating MVAs for the purpose of validating information for a driver's license, permit, or identification card issued by the state MVAs.

K. To the DOJ, Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction of E-Verify, especially with respect to discrimination.

L. To persons and other entities authorized by federal law to determine the employment eligibility of individuals subject to verification under E-Verify (e.g., SSA).

M. To federal government intelligence or counterterrorism agencies or components when DHS becomes aware of a violation or potential violation of E-Verify program requirements that is related to an indication of a threat or potential threat to national security to assist in countering such threat.

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/USCIS stores records in this system electronically or on paper in secure facilities in a locked drawer behind a locked door. The records may be stored on magnetic disc, tape, and digital media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: DHS/USCIS may retrieve records by name, verification case number, A-Number, I-94 Number, Receipt number, Passport (United States or Foreign) number and country of issuance, Driver's License, Permit, or State-Issued Identification Card Number, or SSN of the employee or employee user, or by the submitting company name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: E-Verify records are covered by NARA-approved records retention and disposal schedule, N1-566-08-007. USCIS stores and retains records collected in the process of enrolling in E-Verify and in verifying employment eligibility for ten (10) years from the date of the completion of the last transaction, unless the records are part of an ongoing investigation in which case they may be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud possible using E-Verify (under 18 U.S.C. sec. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship, or naturalization documents).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DHS/USCIS safeguards records in this system according to applicable rules and policies,

including all applicable DHS automated systems security and access policies. USCIS 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: 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 to the USCIS FOIA/Privacy Act Officer whose contact information can be found at http://www.dhs.gov/foia under "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 you may be available under the Freedom of Information Act.

When an individual is seeking records about himself or herself from this system of records or any other Departmental system of records, the individual's request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. The individual must first verify his/her identity, meaning that the individual must provide his/her full name, current address, and date and place of birth. The individual must sign the request, and the individual's 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 believes the Department would have information being requested;
- Identify which component(s) of the Department he or she believes may have the information;
- Specify when the individual believes 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 an individual's request is seeking records pertaining to another living individual, the request must include an authorization from the individual whose record is being requested, authorizing the release to the requester.

Without the above information, the component(s) may not be able to conduct an effective search, and the individual's 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, individuals may make a request for amendment or correction of a record of the Department about the individual by writing directly to the Department component that maintains the record, unless the record is not subject to amendment or correction. The request should identify each particular record in question, state the amendment or correction desired, and state why the individual believes that the record is not accurate, relevant, timely, or complete. The individual may submit any documentation that would be helpful. If the individual believes that the same record is in

more than one system of records, the request should state that and be addressed to each component that maintains a system of records containing the record. For records not covered by the Privacy Act or Judicial Redress Act, individuals may still amend their records at a USCIS Field Office by making an InfoPass appointment http://infopass.uscis.gov_or by contacting the USCIS Contact Center at 1-800-375-5283.

NOTIFICATION PROCEDURES: See "Record Access Procedures."

EXEMPTIONS PROMULGATED FOR THE SYSTEM: No exemption will be claimed except for those records covered by a system of records that have been claimed exempt in that source system identified above in the record source categories under 5 U.S.C. 552a(j)(2) and are covered by this system of records. DHS will claim the same exemptions for those records that are claimed for the original primary systems of records from which they originated for this system.

HISTORY: DHS/USCIS-011 E-Verify Program, 79 FR 46852 (August 11, 2014); E-Verify Program, 77 FR 47419 (August 8, 2012); Verification and Information System (VIS), 73 FR 75445 (December 11, 2008); VIS, 73 FR 10793 (February 28, 2008); VIS, 72 FR 17569 (April 9, 2007); Justice/INS-035, 67 FR 64134 (October 17, 2002); and Alien Status; and Verification Index (ASVI) Justice/INS-009, 66 FR 174 (September 7, 2001).

Jonathan R Cantor,

Acting Chief Privacy Officer,

Department of Homeland Security.

[FR Doc. 2019-12789 Filed: 6/17/2019 8:45 am; Publication Date: 6/18/2019]