League of the United States Building, 2300 Wilson Boulevard, Suite 100, Arlington, VA 22201. The meeting will be open to the public.

DATES: The NIAC will meet on Friday, September 5, 2014, from 1:30 p.m. to 4:30 p.m. The meeting may close early if the council has completed its business. For additional information, please consult the NIAC Web site, *www.dhs.gov/NIAC,* or contact the NIAC Secretariat by phone at (703) 235–2888 or by email at *NIAC@hq.dhs.gov.*

ADDRESSES: Navy League of the United States Building, 2300 Wilson Boulevard, Suite 100, Arlington, VA 22201. For information on facilities or services for individuals with disabilities, or to request special assistance at the meeting, contact the person listed under **FOR FURTHER INFORMATION CONTACT** below as soon as possible.

To facilitate public participation, we are inviting public comment on the issues to be considered by the Council as listed in the ''Summary'' section below. Comments must be submitted in writing no later than 12:00 p.m. on September 2, 2014, must be identified by ''DHS–2014–0036,'' and may be submitted by any *one* of the following methods:

- *Federal eRulemaking Portal: www.regulations.gov.* Follow the instructions for submitting written comments.
- *Email: NIAC@hq.dhs.gov.* Include the docket number in the subject line of the message.
- *Fax:* (703) 603–5098.
- *Mail:* Nancy Wong, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane SW., Mail Stop 0607, Arlington, VA 20598–0607.

Instructions: All written submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Written comments received will be posted without alteration at *www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received by the NIAC, go to *www.regulations.gov.*

Members of the public will have an opportunity to provide oral comments on the Transportation Resilience Working Group study and on Senior Executive/Chief Executive Officer (CEO) Engagement and Summary of the National Infrastructure Protection Plan 2013: *Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013). We request that comments be limited to the issues listed in the meeting agenda and previous NIAC studies. All previous NIAC studies can be located at *www.dhs.gov/NIAC.* Public comments may be submitted in writing or presented in person for the Council to consider. Comments received by Nancy Wong after 12:00 p.m. on September 2, 2014, will still be accepted and reviewed by the members, but not necessarily by the time of the meeting. In-person presentations will be limited to three minutes per speaker, with no more than 15 minutes for all speakers. Parties interested in making in-person comments should register on the Public Comment Registration list available at the meeting location no later than 15 minutes prior to the beginning of the meeting.

FOR FURTHER INFORMATION CONTACT: Nancy Wong, National Infrastructure Advisory Council Designated Federal Officer, Department of Homeland Security, (703) 235–2888.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. App. (Pub. L. 92–463). The NIAC shall provide the President, through the Secretary of Homeland Security, with advice on the security and resilience of the Nation's critical infrastructure sectors.

The NIAC will meet to discuss issues relevant to critical infrastructure security and resilience as directed by the President. At this meeting, the committee will receive and discuss a presentation from the Transportation Resilience Working Group documenting their work to date on a study reviewing the Transportation Sector's resilience against potentially disruptive events. The committee will also receive a working group update on the development of recommendations for an Executive Summary of the National Infrastructure Plan 2013, targeted for use by Senior Executive Level/CEO critical infrastructure owners and operators and a communication strategy with this target community. Both presentations will be posted no later than one week prior to the meeting on the council's public Web page—*www.dhs.gov/NIAC.* The council will review and discuss the presentations, and determine a path forward on each initiative.

Meeting Agenda

I. Opening of Meeting
II. Roll Call of Members
III. Opening Remarks and Introductions
IV. Approval of Meeting Minutes
V. *Working Group Presentation on Transportation Resilience Study, Path Forward to Execute Study*
VI. *Working Group Presentation on Status, and Refinement of Path Forward of Government Requested Recommendation on Senior Executive/CEO Engagement and Executive Summary of the NIPP 2013*
VII. Public Comment: Topics Limited to Transportation Resilience Study; Senior Executive/CEO Engagement and Executive Summary of NIPP 2013; and Previously Issued NIAC Studies and Recommendations
VIII. *Discussion and Deliberations by Council on Presentations and Paths Forward of Working Groups*
IX. Closing Remarks

Nancy Wong,

Designated Federal Officer for the NIAC.

[FR Doc. 2014–18871 Filed 8–8–14; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2014–0040]

Privacy Act of 1974; Department of Homeland Security U.S. Citizenship and Immigration Services—011 E-Verify Program System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to update and reissue a current Department of Homeland Security system of records titled, ''Department of Homeland Security/U.S. Citizenship and Immigration Services—011 E-Verify Program System of Records.'' The U.S. Citizenship and Immigration Services E-Verify program allows employers to electronically verify the employment authorization of newly hired employees. To provide individuals the ability to learn about their work authorization status information, the U.S. Citizenship and Immigration Services also operates a free service called Self-Check. The U.S. Citizenship and Immigration Services is launching enhanced features to the Self Check service that permits individuals who successfully complete a Self Check identification process the opportunity to establish a myE-Verify account. The information collected to register and maintain a myE-Verify account is covered by the ''Department of Homeland Security/ALL—037 E-Authentication System of Records''

published elsewhere in the **Federal Register**. U.S. Citizenship and Immigration Services is updating this System of Records Notice to include the operational data previously covered by ''Department of Homeland Security U.S. Citizenship and Immigration Services—013 Self Check System of Records,'' which is being consolidated into DHS/ALL—037 E-Authentication System of Records and this System of Records Notice. The Self Check query, query results, and Self Lock transaction history will now be maintained by this updated System of Records Notice. The initial launch of myE-Verify will allow access to a feature called ''Self Lock,'' which enables an account holder to prevent the use of his or her Social Security number in E-Verify and Self Check. Additional myE-Verify account features such as Case History, Case Tracker, and Document Expiration Reminders will be made available in future releases. The Department of Homeland Security is updating this Privacy Act System of Records Notice for the E-Verify Program in order to provide notice that E-Verify is updating the ''Category of Individuals,'' ''Category of Records,'' ''Purpose(s),'' and ''Record Source Categories'' to account for additional information necessary to operate myE-Verify account features. E-Verify is updating the ''Category of Individuals'' to include individuals that successfully use the E-Verify Self Check service to check employment eligibility, which was previously covered by the E-Verify Self Check System of Records, and individuals who have locked their Social Security number in E-Verify. E-Verify is also updating the ''Category of Records'' to include Self Check query information, which was previously covered by the E-Verify Self Check System of Records Notice, and Social Security number lock information. E-Verify is updating the ''Purpose(s)'' to include providing employment authorization information to individuals seeking to check employment eligibility under the Immigration and Naturalization Act. This system will also enable individuals to access features concerning the use of their personally identifiable information in E-Verify and Self Check, such as the ability to lock their Social Security number to prevent its use in E-Verify and Self Check.

This updated system will be included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before September 10, 2014. This updated system will be effective September 10, 2014.

ADDRESSES: You may submit comments, identified by docket number DHS–2014–0040 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: Karen Neuman, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

Instructions: All submissions received must include the agency name and docket number for this rulemaking. 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, please visit *http://www.regulations.gov*.

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Donald K. Hawkins, (202) 272–8030, Privacy Officer, U.S. Citizenship and Immigration Services, 20 Massachusetts Avenue NW., 5th Floor, Washington, DC 20529. For privacy questions, please contact: Karen Neuman, (202) 343–1717, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, DC 20528.

SUPPLEMENTARY INFORMATION:

I. Background

In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, the Department of Homeland Security (DHS) U.S. Citizenship and Immigration Services (USCIS) proposes to update and reissue a current DHS system of records titled, ''DHS/USCIS–011 E-Verify Program System of Records.'' The USCIS E-Verify Program allows employers to confirm employment eligibility of newly hired employees.

To provide individuals the ability to learn about their work authorization status information, USCIS operates a free service called Self-Check. USCIS is launching enhanced features to the Self Check service that permit 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 the ''DHS/ALL–037 E-Authentication System of Records'' published elsewhere in the **Federal Register**. DHS/ALL–037 E-Authentication System of Records and this System of Records Notice consolidate the previously issued ''Department of Homeland Security U.S. Citizenship and Immigration Services-013 Self Check System of Records.'' As a result of this consolidation, by this notice, DHS intends to remove DHS/USCIS–013 from its inventory of systems of records.

The initial launch of myE-Verify will allow access to a feature called ''Self Lock,'' which will enable an account holder to prevent the use of his or her Social Security number (SSN) in E-Verify and Self Check. Additional myE-Verify account features such as Case History, Case Tracker, and Document Expiration Reminders will be made available in future releases. DHS is updating this Privacy Act System of Records Notice for the E-Verify Program to provide notice that E-Verify is updating the ''Category of Individuals,'' ''Category of Records,'' ''Purpose(s),'' and ''Record Source Categories'' to account for the additional information collection necessary to operate myE-Verify account features. E-Verify is updating the ''Category of Individuals'' to include (1) individuals that successfully use the E-Verify Self Check service to check employment eligibility, which was previously covered by the E-Verify Self Check System of Records, and (2) individuals who have locked their SSN in E-Verify. E-Verify is also updating the ''Category of Records'' to include (1) Self Check query information, which was previously covered by the E-Verify Self Check System of Records Notice, and (2) SSN lock information. E-Verify is updating ''Purpose(s)'' to include providing employment authorization information to individuals seeking to check employment eligibility under the Immigration and Naturalization Act. This system will also enable individuals to access features concerning the use of their personally identifiable information in E-Verify and Self Check such as the ability to lock their SSN to prevent its use in E-Verify and Self Check.

This updated 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. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals when systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors.

Below is the description of the DHS/USCIS–011 E-Verify Program System of Records.

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

System of Records

Department of Homeland Security (DHS)/U.S. Citizenship and Immigration Services (USCIS)–011.

SYSTEM NAME:

DHS/USCIS–011 E-Verify Program.

SECURITY CLASSIFICATION:

Unclassified, for official use only.

SYSTEM LOCATION:

Records are maintained at USCIS Headquarters in Washington, DC, field offices, and at the DHS Stennis Data Center (DC1).

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by the E-Verify program include: Employees, both U.S. Citizens and non-U.S. Citizens, whose employers have submitted to E-Verify their identification and contact information; employers that enroll in E-Verify; designated agents who enroll in E-Verify; individuals employed or retained by employers or designated agents who have accounts to use E-Verify; individuals who contact E-Verify with information on the use of E-Verify; individuals who provide their names and contact information to E-Verify for notification or contact purposes; individuals seeking to check employment eligibility under the Immigration and Naturalization Act (INA); and individuals who have created a myE-Verify account and locked their SSNs in E-Verify to prevent them from being used in E-Verify and Self Check.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. Information about the employee to be verified:

- Name (last, first, middle initial, other names used, if any);
- Date of Birth;
- SSN;
- Contact information such as email address and telephone number;
- Date of Hire;
- Claimed Citizenship Status;
- Acceptable Form I–9 document type;
- 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 if issued by a state or jurisdiction participating in the Records and Information from Departments of Motor Vehicles for E-Verify (RIDE) program and when a Memorandum of Agreement (MOA) exists between the state or jurisdiction and DHS USCIS to verify the information about the document;
- Receipt Number;
- Visa Number;
- A-Number;
- I–94 Number;
- Employment Authorization Document (Form I–766) Number; and
- Permanent Residence Card (Form I–551) Number Photographs, if required by secondary verification.

B. Disposition data from the employer. The following codes are entered by the employer based on what the employer does as a result of the employment verification information (the most up-to-date disposition codes can be found in the E-Verify Employer Manual available at *http://www.dhs.gov/E-Verify*):

- The employee continues to work for the employer after receiving an Employment Authorized result: Employer selects this option based on receiving an Employment Authorized response from E-Verify;
- The employee continues to work for the employer after receiving a Final Non-confirmation (FNC) result: Employer selects this option based on the employee getting an FNC despite the employee contesting the Tentative Non-confirmation (TNC) and the employer retains the employee;
- The employee continues to work for the employer after receiving a No Show result: Employer selects this option based on the employee getting a TNC but the employee did not try to resolve the issue with the Social Security Administration (SSA) or DHS and the employer retains the employee;
- The employee continues to work for the employer after choosing not to contest a TNC: Employer selects this option when the employee does not contest the TNC but the employer retains the employee;
- The employee was terminated by the employer for receiving a FNC result: Employer selects this option when employee receives FNC and is terminated;
- The employee was terminated by the employer for receiving a No Show result: Employer selects this option when employee did not take an action to resolve and is terminated;
- The employee was terminated by the employer for choosing not to contest a TNC: Employer selects this option when employee does not contest the TNC and is terminated;
- The employee voluntarily quit working for the employer: Employer selects this option when employee voluntarily quits job without regard to E-Verify;
- The employee was terminated by the employer for reasons other than E-Verify: Employer selects this option when employee is terminated for reasons other than E-Verify;
- The case is invalid because another case with the same data already exists: Employer selects this option when the employer ran an invalid query because the information had already been submitted; and
- The case is invalid because the data entered is incorrect: Employer selects this option when the employer ran an invalid query because the information was incorrect.
- 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;
- Other.

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

- Company Name;
- Street Address;
- Employer Identification Number;
- 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 Employer User of E-Verify: (e.g., Human Resource employee conducting E-Verify queries):

- Last Name;
- First Name;
- Middle Initial;
- Phone Number;
- 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 Employer Manual available at *http://www.dhs.gov/E-Verify*):
- Employment Authorized,
- DHS Verification in Process,
- SSA TNC,
- DHS TNC,
- Employee Referred to SSA,
- Employee Referred to DHS,
- SSA Case in Continuance (In rare cases SSA needs more than 10 federal government workdays to confirm employment eligibility),
- DHS Case in Continuance (In rare cases DHS needs more than 10 federal government workdays to confirm employment eligibility),
- SSA FNC,
- DHS FNC,
- DHS No Show,
- Case Incomplete,
- Photo Matching Required,
- Review and Update Employee Data, and
- Error: Close Case and Resubmit.

F. Information from state Motor Vehicle Agencies (MVA) used to verify the information from a driver's license, permit, or state issued ID card if the state has established a MOA with DHS USCIS to allow verification of this information. The categories of records from MVAs may include:

- Last Name;
- First Name;
- State or Jurisdiction of Issuance;
- Document Type;
- Document Number;
- Date of Birth;
- Status Text;
- Status Description Text; and
- Expiration Date.

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

- Last Name;
- First Name;
- Middle Name;
- Other Names Used (e.g., Maiden Name);
- Date of Birth;
- Age;
- Country of Birth;
- Country of Citizenship;
- Alien Number;
- SSN;
- Citizenship Number;
- Receipt Number;
- Address;
- Previous Address;
- Phone Number;
- Nationality;
- Gender;
- Photograph;
- Date Entered United States;
- Class of Admission;
- File Control Office Code;
- Form I–94 Number;
- Provision of Law Cited for Employment Authorization;
- Office Code Where the Authorization Was Granted;
- Date Employment Authorization Decision Issued;
- Date Employment Authorization Begins;
- Date Employment Authorization Expires;
- Date Employment Authorization 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 Admitted Until;
- Port of Entry;
- Departure Date;
- Visa Number;
- Passport Number;
- Passport Information including Country of Issuance (COI);
- Passport Card Number;
- Form Number, for example Form I–551 (Lawful Permanent Resident card) or Form I–766 (Employment Authorization Document);
- Expiration Date;
- Employment Authorization Card Information;
- Lawful Permanent Resident Card Information;
- Petitioner Internal Revenue Service Number;
- Class of Admission;
- 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);
- Federal Bureau of Investigation Number;
- Admission Number;
- Petitioner Firm Name;
- Petitioner Tax Number;
- Date of Admission;
- Marital Status;
- Marriage Date and Place;
- Marriage Information and Certificate;
- Visa Control Number;
- Visa Foil Number;
- Class of Admission;
- Case History;
- Alerts;
- Case Summary Comments;
- Case Category;
- Date of Encounter;
- Encounter Information;
- Case Actions & 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 that successfully complete an E-Verify query using Self Check:

- Name (last, first, middle initial, and other names used, if any);
- Date of Birth;
- SSN; and
- Document(s) type, associated number, and associated expiration date that demonstrates work authorization. These may include U.S. Passport, employment authorization document, I–495 Lawful Permanent Resident card, or other documents and associated numbers a listed as acceptable Form I–9 verification documents.

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

- Name (last, first);
- SSN;
- Date of Birth;
- Lock Receipt Number;
- Lock Date and Expiration Date;
- Email Address; and
- Self-Generated Security Questions and Answers.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authority for having a system for verification of employment eligibility is found in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208, §§ 401–405 (Sept. 30, 1996), codified at 8 U.S.C. 1324a note.

PURPOSE(S):

This system provides employment authorization information to employers

participating in E-Verify and to individuals seeking to check employment eligibility under the INA. This system will also enable individuals to access features concerning the use of their personally identifiable information in E-Verify and Self Check such as the ability to lock their SSN to prevent its use in E-Verify and Self Check. It may also be used to support 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 violation of privacy laws or other illegal activity related to misuse of E-Verify, including:

- Investigating duplicate or incomplete enrollments by employers;
- Inappropriate enrollments by individuals posing as employers;
- Verifications that are not performed within the required time limits; and
- Cases referred by and between E-Verify and the Department of Justice Office of Special Counsel for Immigration-Related Unfair Employment Practices, or other 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.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside DHS, except as limited by statute, as a routine use pursuant to 5 U.S.C. 552a(b)(3). Any disclosure of information must be made consistent with the official duties of the person making the disclosure. The routine uses are as follows:

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 of DHS in his/her official capacity;

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

4. the U.S. 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. 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 the security or confidentiality of information in the system of records has been compromised;

2. DHS has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by DHS or another agency or entity) or harm to the individual that rely upon the compromised information; 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 compromise and prevent, minimize, or remedy such harm.

F. 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.

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 the E-Verify program, which includes potential fraud, discrimination, or employment based identity theft and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To employers participating in the E-Verify program in order to verify the employment eligibility of their employees working in the United States.

I. To the American Association of Motor Vehicle Administrators Network and participating MVAs for the purpose of validating information for a driver's license, permit, or identification card issued by the Motor Vehicle Agency of states or jurisdictions who have signed a Memorandum of Agreement with DHS under the RIDE program.

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

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 or when disclosure is necessary to preserve confidence in the integrity of DHS, or 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 an unwarranted invasion of personal privacy.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

None.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:

Records in this system are stored electronically or on paper in secure facilities in a locked drawer behind a locked door. The records are stored on magnetic disc, tape, digital media, and CD–ROM.

RETRIEVABILITY:

Records may be retrieved by name, verification case number, Alien Number, I–94 Number, Receipt Number, Passport (U.S. or Foreign) Number and COI, Driver's License, Permit, or State-Issued Identification Card Number, or SSN of the employee, employee user, or by the submitting company name.

SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable rules and policies, including all applicable DHS automated systems security and access policies. Strict controls have been imposed 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.

RETENTION AND DISPOSAL:

NARA approved the retention and disposal schedule, N1–566–08–007, which covers E-Verify records. E-Verify 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. § 3291, the statute of limitations for false statements or misuse regarding passports, citizenship, or naturalization documents).

SYSTEM MANAGER AND ADDRESS:

Chief, Verification Division, USCIS, Washington, DC 20528.

NOTIFICATION PROCEDURE:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the USCIS, Freedom of Information Act (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 himself or herself, the individual may submit the request to the Chief Privacy Officer and Chief Freedom of Information Act Officer, Department of Homeland Security, 245 Murray Drive SW., Building 410, STOP–0655, Washington, DC 20528.

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

- Explain why you believe the Department would have information on you;
- Identify which component(s) of the Department you believe may have the information about you;
- 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 your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his/her agreement for you to access his/her records. Without the above information the component(s) may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

RECORD ACCESS PROCEDURES:

See ''Notification procedure'' above.

CONTESTING RECORD PROCEDURES:

See ''Notification procedure'' above.

RECORD SOURCE CATEGORIES:

Records are obtained from several sources including:

(A) Information collected from employers about their employees relating to employment eligibility verification;

(B) Information collected from E-Verify users used to provide account access and monitoring;

(C) Information collected from Federal and state databases listed below:

- SSA Numident System,
- Customs and Border Protection (CBP) Arrival and Departure Information System (ADIS),
- CBP Nonimmigrant Information System (NIIS) and Border Crossing Information (BCI),
- Immigration Customs and Enforcement (ICE) Student and Exchange Visitor Identification System (SEVIS),
- ICE ENFORCE Integrated Database (EID) Enforcement Alien Removal, Module (EARM) Alien Number,
- USCIS Aliens Change of Address System (AR–11),
- USCIS Central Index System (CIS),
- USCIS Customer Profile Management System (CPMS),
- USCIS Computer-Linked Application Information Management System Version 3 (CLAIMS 3),
- USCIS Computer-Linked Application Information Management System Version 4 (CLAIMS 4),
- USCIS Citizenship and Immigration Services Centralized Operational Repository (CISCOR),
- USCIS National File Tracking System (NFTS),
- USCIS Microfilm Digitization Application System (MiDAS),
- USCIS Marriage Fraud Amendment System (MFAS),
- USCIS Enterprise Document Management System (EDMS),
- USCIS Refugees, Asylum, and Parole System (RAPS),
- Department of State Consular Consolidated Database (CCD),
- DOJ EOIR Case Access System,
- State Motor Vehicle Administrations, if participating in the E-Verify RIDE initiative,

(D) Information created by E-Verify, and

(E) Information from individuals seeking to check employment eligibility and access to features concerning the use of their information in E-Verify and Self Check.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: July 31, 2014.

Karen L. Neuman,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2014–18701 Filed 8–8–14; 8:45 am]

BILLING CODE 9111–97–P

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2014–0039]

Privacy Act of 1974; Department of Homeland Security/ALL–037 E-Authentication Records System of Records

AGENCY: Privacy Office, Department of Homeland Security.

ACTION: Notice of Privacy Act System of Records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Homeland Security proposes to establish a new system of records titled, Department of Homeland Security/ALL–037 E-Authentication Records System of Records. This system of records allows the Department of Homeland Security to collect, maintain, and retrieve records about individuals, including members of the public, who electronically authenticate their identities. The information in this system of records includes data collected by programs and applications for use when the Department of Homeland Security or a