DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS–2011–0030]

Privacy Act of 1974; Department of Homeland Security/United States Citizenship and Immigration Services—DHS/USCIS–011 E-Verify Program System of Records

AGENCY: Privacy Office, DHS.

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/United States Citizenship and Immigration Services—011 E-Verify Program System of Records." The United States Citizenship and Immigration Services E-Verify Program allows employers to check citizenship status and verify employment eligibility of newly hired employees. 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: (1) Adding a new category of records derived from participating Motor Vehicle Agencies' systems through the American Association of Motor Vehicle Administrators Network; (2) adding a new category of records derived from individual employees subject to employment verification; and (3) changing the verification process to include the validation of information from a driver's license, driver's permit, or identification card from a state or jurisdiction that has signed a Memorandum of Agreement with the Department of Homeland Security under the Records and Information from Departments of Motor Vehicles for E-Verify program. These changes are more thoroughly spelled out in an accompanying E-Verify Privacy Impact Assessment update, which is found on the Department of Homeland Security Privacy Web site (*http://www.dhs.gov/privacy*). This updated system is included in the Department of Homeland Security's inventory of record systems.

DATES: Submit comments on or before June 8, 2011. This updated system will be effective June 8, 2011.

ADDRESSES: You may submit comments, identified by docket number DHS–2011–0030 by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Fax:* 703–483–2999.
- *Mail:* Mary Ellen Callahan, 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 go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: For general questions, please contact: Janice Jackson, Acting Privacy Branch Chief, Verification Division, U.S. Citizenship and Immigration Services, Department of Homeland Security, Washington, DC 20528. For privacy issues please contact: Mary Ellen Callahan (703–235–0780), 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) United States 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 check citizenship status and verify employment eligibility of newly hired employees. DHS is updating this Privacy Act System of Records Notice for the E-Verify Program in order to provide notice that E-Verify is: (1) Adding a new category of records derived from participating Motor Vehicle Agencies' (MVA) systems through the American Association of Motor Vehicle Administrators Network (AAMVAnet™); (2) adding a new category of records derived from individual employees subject to employment verification; and (3) changing the verification process to include the validation of information from a driver's license, driver's permit, or identification card from states or jurisdictions that have signed a Memorandum of Agreement (MOA) with DHS USCIS under the AAMVAnet™ Records and Information from Departments of Motor Vehicles for E-Verify (RIDE) program.

E-Verify is mandated by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law (Pub. L.) 104–208, September 30, 1996. The program is a free and, in most cases, voluntary DHS program implemented by USCIS and operated in collaboration with the Social Security Administration (SSA). The program compares information provided by employees on the Employment Eligibility Verification Form (Form I–9) against information in SSA and DHS databases in order to verify an employee's employment eligibility.

All U.S. employers are responsible for the completion and retention of Form I–9 for each individual, whether citizen or non-citizen, they hire for employment in the United States. On Form I–9, the employer must verify the employment eligibility and identity documents presented by the employee and record the document information on Form I–9.

The Immigration and Naturalization Service (INS) initially developed the predecessor to E-Verify, the Basic Pilot Program, as a voluntary pilot program as required by IIRIRA. When Congress created DHS, it incorporated INS programs under DHS and USCIS was charged with operating the Basic Pilot Program. In addition to changing the name of the Basic Pilot Program, USCIS has continued to develop the program as the requirements for employment verification have changed over time. The program is in most cases voluntary. However, both Federal employees and those employees working on Federal contracts are required to have their work authorization eligibility verified by E-Verify. Contractors have the discretion to verify all employees through E-Verify whether or not they are working on Federal contracts. In addition, some states require the use of E-Verify for state employees while others require its use by all employers located within their state or by all state job services.

E-Verify is a fully operational, Web-based program that allows any employer to enroll and verify employees' employment eligibility.

DHS is updating and reissuing the E-Verify SORN to provide notice of the additional data that may be used by E-Verify in the verification process, specifically the automation of motor vehicle document verification between MVAs and E-Verify employers through the RIDE initiative.

The RIDE initiative enhances E-Verify by providing employers the ability to validate information from the most commonly presented identity documents for employment authorization: An employee's driver's license, driver's permit, or state-issued identification card, against MVA data

when the issuing state or jurisdiction of those documents has established an MOA with DHS USCIS to participate in RIDE and allow verification of this information.

Currently, E-Verify collects only limited information about documents presented during the Form I–9 and E-Verify process; however, this is limited to U.S. Passports and documents presented by Non-U.S. Citizens. For other documents, E-Verify collects only the documents presented from list B & C of the Form I–9 Lists of Acceptable Documents. An example of a Form I–9 List B document is a driver's license or state issued identification card. An example of a Form I–9 List C document is a Social Security card or certified birth certificate.

If an individual presents a document from list B & C of the Form I–9, E-Verify will now also collect the document type, expiration date, and the state or jurisdiction of issuance. In addition, E-Verify will collect the document number in cases where an MOA exists between the issuing state or jurisdiction and DHS USCIS. E-Verify collects the document expiration date in order to determine whether the individual presented an unexpired identity document in order to meet the Form I–9 requirement. E-Verify collects the issuing state or jurisdiction of the document to direct its query to the appropriate MVA database for validation of the document's information, and to project potential workload as additional states sign on to participate in RIDE. E-Verify collects the document type for each case to project potential workload as additional states sign MOAs with DHS USCIS to participate in RIDE. E-Verify collects the document number to validate information from the document presented with the issuing MVA and only in cases where the issuing state or jurisdiction has established an MOA with DHS USCIS to do so.

The RIDE initiative, including the associated Tentative Non-Confirmation (TNC) process, is more fully discussed in the description of the E-Verify process below.

The addition of the RIDE functionality to E-Verify is an important step in ensuring that individuals do not gain employment authorization through the misuse of state-issued identity documents in E-Verify.

The following describes the complete E-Verify process, including the new RIDE enhancement.

Enrollment

E-Verify participants may be one of two different classes of user types: (1) Employers who use E-Verify for their own employees; or (2) designated agents who use E-Verify for the employees of other companies. Employer agents (previously called designated agents) usually query E-Verify as a commercial service for other employers that cannot, or choose not, to conduct the E-Verify queries but who want the benefit of the program. To use E-Verify, employers and employer agents must first enroll their company online at *http://www.dhs.gov/E-Verify.* They complete a registration application that collects basic contact information including: Company name, company street address, employer identification number, North American Industry Classification System (NAICS) Code, number of employees, number of employment sites, parent company or corporate company, name of company Point of Contact (POC) for E-Verify Usage, POC phone number, POC fax number, and POC e-mail address.

Participants, whether an employer or employer agent, can then create user accounts for the employees who have access to E-Verify. A user may be one of three user types:

- *General User:* This user type performs verification queries, views reports, and has the capability to update their personal user account.
- *Program Administrator:* This user type is responsible for creating user accounts at their site for other Program Administrators and General Users. They have the responsibility to view reports, perform queries, update account information, and unlock user accounts if a user has locked the account by entering the wrong password.
- *Corporate Administrator:* This user type can view reports for all companies associated with the E-Verify corporate account. This allows them to see the activities associated with each general user. They can also update user accounts, register new locations and users, terminate access for existing locations, and perform site and user maintenance activities for all sites and users associated with the corporate account. Each company can have a single corporate administrator.

E-Verify collects information about the user so that the program can review and identify the use of the system by employers, and allows the program to see more detailed information about user system usage. The information collected specifically on users includes: Name (last, first, middle initial), phone number, fax number, e-mail address, and User ID.

Every E-Verify participating employer is required to read and sign a Memorandum of Understanding (MOU) that explains the responsibilities of DHS, SSA, and the participant. Once the E-Verify participant has completed the enrollment form, E-Verify e-mails a unique user login and password to the user. The employer must conspicuously display E-Verify posters (posters are found on the Web site and are printed out by each employer) at the hiring site that indicate the employer's participation in E-Verify and describe the employees' rights regarding the employer's participation in the program.

E-Verify Verification Process

Once employers enroll in E-Verify, they must verify the employment eligibility of all new employees hired thereafter by entering the employee's name, date of birth (DOB), Social Security Number (SSN), and information about the documents provided by the employee during the Form I–9 process, into the E-Verify online user interface tool. For some documents presented during the Form I–9 process, E-Verify also collects the expiration date as entered by the employer and compares it against the hire date entered by the employer to make sure that the document is unexpired. Due to the fact that employers can now enter hire dates up to 365 days in the future in E-Verify, the document is still acceptable if it is expired on the future date of hire—the day an employee starts work for pay—so long as it is unexpired on the day the case is initiated. Additionally, if the employer enters into E-Verify that the employee provided a driver's license, driver's permit, or state-issued ID card as the document to establish identify on the Form I–9, then E-Verify will request that the employer enter the type of document presented, as well as the state of issuance and expiration date. The expiration date is then validated by E-Verify to ensure that an unexpired document was presented by the employee to the employer. If the document presented was issued by a state or jurisdiction participating in RIDE, then E-Verify also collects and verifies the document number as described below.

Form I–9 contains a field for the SSN, but the employee is not required to provide this number unless the employer is participating in E-Verify. All employers in the United States are required to use this form regardless of whether they are enrolled in E-Verify.

Processing Non-U.S. Citizens

For Non-U.S. Citizens, including immigrants, non-immigrants, and lawful permanent residents, the vast majority of queries are completed when E-Verify

verifies the name, SSN, and DOB against the SSA NUMIDENT System (71 FR 1796), followed by the name, DOB, and Form I–9 identity document information against certain DHS and MVA databases when the state or jurisdiction is participating in RIDE. The specific database against which the information will be verified depends on the document provided by the employee. For example, if the employee uses an Employment Authorization Document (EAD), the Alien Number (hereafter "A–Number") is queried against the USCIS Central Index System (CIS), and the EAD photograph, as described below against the USCIS Image Storage and Retrieval System (ISRS). If the employee is a non-immigrant, E-Verify queries the Arrival Departure Record (Form I–94) number against the United States Customs and Border Protection (CBP) Non Immigrant Information System (73 FR 77739) and Border Crossing Information System (73 FR 43457). If the employee provides a driver's license, driver's permit, or state-issued ID card and the issuing state or jurisdiction is a participant in RIDE, and an MOA exists between the state or jurisdiction and DHS USCIS to validate the information, then E-Verify verifies that document against the participating MVA's database. If SSA, DHS, and the state MVA database (if applicable) are able to verify the employee's employment eligibility, the employer receives an Employment Authorized (EA) notification. E-Verify generates a case verification number and the employer may either print and retain the Case Details page from E-Verify or write the case verification number on Form I–9.

If the automated query does not immediately result in an EA response from E-Verify, the employer receives Verification in Process response, which means that the query has been automatically sent to the USCIS status verifiers. The USCIS status verifiers have one day to verify the employee's employment eligibility by manually reviewing the information submitted by the employer against information in DHS, the U.S. Department of State (DoS), and SSA databases. USCIS status verifiers are trained to evaluate the information provided by the employee against the various DHS databases. This could not be done as an automated process because of the complexities of the various types of data. If the USCIS status verifiers are able to confirm employment eligibility with the information available to them, they indicate the response in E-Verify and the employer receives the EA notification.

If the USCIS status verifiers are unable to confirm employment eligibility, E-Verify displays a DHS Tentative Non-Confirmation (TNC) response and generates a TNC notice for the employer to print and give to the employee that explains that the employee has received a TNC without going into detail about specifically what caused the TNC. The notice also explains the employee's rights, including the right to contest the result with DHS. If the employee wishes to contest the TNC, he/she must notify his employer.The employer then indicates the employee's wish to contest the TNC in E-Verify, upon which E-Verify generates a Referral Letter. This letter instructs the employee that he has eight days to contact USCIS status verifiers to resolve the discrepancy. Once the employee contacts the USCIS status verifiers, the USCIS status verifiers attempt to resolve the discrepancy by either requesting that the employee submit copies of the employee's immigration documents or by researching a number of DHS or DoS databases to determine whether there is additional information pertaining to that individual that would confirm the employment eligibility status. To conduct these database searches, USCIS status verifiers use a Person Centric Query System (PCQS) to facilitate the information search. If the USCIS status verifier determines that the employee is eligible to work, the USCIS status verifier indicates this in E-Verify. The E-Verify system then notifies the employer that the employee is EA. If the USCIS status verifier determines that an employee is not eligible to work, the USCIS status verifier updates E-Verify with a Final Non-Confirmation (FNC) disposition and E-Verify notifies the employer of this resolution. At this point, the employer may legally terminate the individual's employment and the employer must update the system to acknowledge any action taken. If an employer retains an employee who has received FNC that he is not eligible to work, it must notify DHS that it will retain the employee. If the employer fails to notify DHS, the employer may be liable for failure to notify and knowingly employing an individual who is not eligible to work.

Records and Information From Department of Motor Vehicles for E-Verify (RIDE)

The RIDE process begins when an employer indicates in E-Verify that an employee has presented a List B document on the Form I–9 (*e.g.* driver's license, driver's permit, or valid ID card). E-Verify first prompts the employer for the document type (driver's license, driver's permit, or state-issued ID card) and state of issuance. If E-Verify determines that the state of issuance and the document type is one that can be validated for RIDE (per the MOA between the MVA and DHS USCIS), E-Verify prompts the employer for: Employee name, employee DOB, employee SSN, hire date, document number, and document expiration date as provided on Form I–9. If E-Verify cannot verify the information provided under RIDE because there is not an existing MOA, then E-Verify collects the same information with the exception of the document number, since the document will not be verified against an MVA database.

E-Verify determines if the expiration date of the driver's license, driver's permit, or state-issued ID card as entered by the employer indicates that the employee presented an unexpired document to the employer. If E-Verify determines that an expired document was presented, E-Verify prompts the employer to enter a document that was not expired on the date of hire.

Next, the SSA validation, which is a standard part of the current E-Verify process, begins. E-Verify sends the SSN, citizenship status, name, and DOB to SSA for validation. If SSA does not validate the case information, E-Verify issues a TNC at that point and no further transactions occur until the TNC is resolved with SSA.

Once the query successfully passes SSA validation, E-Verify sends relevant license information (DOB, document number) to the state MVA database. The MVA returns a portion of the MVA record relevant to that document to E-Verify. Due to differences in MVA databases, variations in data returned to E-Verify by participating MVAs may occur. A complete list of states and jurisdictions participating in RIDE and the documents which are being verified is available in Appendix A of the E-Verify PIA update which is publishing concurrently with this SORN and available at *http://www.dhs.gov/privacy.* E-Verify compares the MVA information to the information initially entered by the employer to determine if there is a match between the document number and DOB provided by the MVA database and the document number and DOB entered by the employer. The employer does not see the MVA record, and will only see the final response given by E-Verify either EA or TNC if there is no match.

E-Verify issues an EA response if it determines a match at this step of the process. The employer does not see any

additional driver's license or identity information from the MVA or E-Verify, only the resulting response of EA, or TNC if there is no match.

If the MVA cannot find a matching record or E-Verify cannot match the document number and DOB based on the record returned by the MVA, E-Verify instructs the employer to check and, if necessary, correct the document number and/or DOB fields and resubmit the information through E-Verify. E-Verify matches the record by document number and DOB only; these are the only fields that can be changed by the employer. There is no name matching in the RIDE process. If after the second attempt there is still no match, the employer receives notice that the employee was issued a DHS TNC.

As with any E-Verify TNC, the employer must share the result with the employee, who has the option of whether or not to contest. If the employee chooses to contest, the employer prints a referral letter, which provides directions to the employee on how to contest the TNC. This letter instructs the employee that he has eight days to contact a USCIS status verifier to resolve the discrepancy.

If a TNC is generated because of a RIDE mismatch and the individual chooses to contest the TNC, the employee must call a USCIS status verifier and fax in a copy of the document (*e.g.,* driver's license) provided to establish identity on Form I–9. USCIS status verifiers compare the faxed copy of the document with the information in the MVA's database via the PCQS. Status Verifiers use PCQS to conduct manual queries of databases for status verification; in this case, the MVA database of the issuing state or jurisdiction. As in other TNCs, the status verifier attempts to resolve the TNC within 24 hours. If the USCIS status verifier is unable to match the driver's license, the status verifier places the case in continuance and contacts the MVA to determine whether it is a true mismatch or an error in the MVA database. This process ensures that all contested TNCs receive a full examination against the MVA's records in order to avoid issuing a FNC because the MVA database was incorrect or because the document contained errors. Once the status verifier has researched the document, he enters a response that triggers an update to the case in E-Verify. E-Verify will display a response of EA or FNC to the employer depending on the resolution. If the employee chooses not to contest the TNC or does not contact a USCIS status verifier within eight Federal workdays, E-Verify automatically issues an FNC.

Photo Screening Tool

In addition to the normal verification process, if the employee has used certain DHS-issued documents, such as the Permanent Resident Card (Form I–551) or the Employment Authorization Card (Form I–766), or if the employee is a U.S. Citizen who used a U.S. passport for completing Form I–9, the E-Verify tool presents the photo on record for the applicable document to the employer. The DHS photos come from USCIS's ISRS database, and the passport photos come from a copy of the DoS passport data contained in TECS, the information technology system maintained by CBP. This feature is known as the Photo Screening Tool. The employer visually compares the photo presented by E-Verify with the photo on the employee's card. The two photos should be an exact match. (This is not a check between the individual and the photo on the card, since the employer compares the individual to their photo ID during the Form I–9 process.) The employer must then indicate in E-Verify whether the pictures match or not. Depending on the employer's input, this may result in an EA response, or a DHS TNC for the employee based on a photo mismatch, which the employee will need to resolve by contacting a USCIS status verifier. If the employer reports a mismatch that results in a TNC, the employee is notified that he needs to provide a photocopy of their document to a USCIS status verifier. The USCIS status verifier does various searches to try to confirm the information supplied by the employee. In cases where the USCIS status verifier cannot match the information because the employee is asserting that there is a mistake in the document, the employee is directed to their local USCIS Application Support Center for resolution.

E-Verify User Rules and Restrictions

E-Verify provides extensive guidance for the employer to operate the E-Verify program through the user manual and training. One of the requirements for using E-Verify is that the employer must only submit an E-Verify query after hiring an employee. Further, the employer must perform E-Verify queries for newly hired employees no later than the third business day after they start work for pay. These requirements help to prevent employers from misusing the system.

While E-Verify primarily uses the information it collects for verification of employment eligibility, the information may also be used for law enforcement (to prevent fraud and misuse of E-Verify, and to prevent discrimination and identity theft), program analysis, monitoring and compliance, program outreach, customer service, and prevention of fraud or discrimination. On a case-by-case basis, E-Verify may give law enforcement agencies extracts of information indicating potential fraud, discrimination, or other illegal activities. The USCIS Verification Division uses information contained in E-Verify for several purposes:

(1) Program management, which may include documentary repositories of business information, internal and external audits, congressional requests, and program reports;

(2) Data analysis for program improvement efforts and system enhancement planning, which may include conducting surveys, user interviews, responding to public comments received during rulemakings or from call center contacts which may make outgoing or receive incoming calls regarding E-Verify, including using information for testing purposes;

(3) Monitoring and compliance, as well as quality assurance efforts, which may include analysis of customer use, data quality, or possible fraud, discrimination or misuse or abuse of the E-Verify system. This may originate directly from E-Verify;

(4) Outreach activities to ensure adequate resources are available to current and prospective program participants, which may include call lists and other correspondence. USCIS may also permit designated agents and employers to use the E-Verify logo if they have agreed to certain licensing restrictions;

(5) Customer service enhancements to improve the user's experience while using E-Verify; and

(6) Activities in support of law enforcement to prevent fraud and misuse of E-Verify, and to prevent discrimination and identity theft.

This System of Records Notice is replacing the System of Records Notice previously published in the **Federal Register** on May 19, 2010 (75 FR 28035).

II. Privacy Act

The Privacy Act embodies fair information principles in a statutory framework governing the means by which the United States Government collects, maintains, uses, and disseminates 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 for 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 where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR part 5.

The Privacy Act requires each agency to publish in the **Federal Register** a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to their records are put, and to assist individuals to more easily find such files within the agency. 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)/United States Citizenship and Immigration Service (USCIS)—011.

SYSTEM NAME:

Department of Homeland Security/United States Citizenship Immigration Services—011 E-Verify Program System of Records.

SECURITY CLASSIFICATION:

Unclassified, for official use only.

SYSTEM LOCATION:

Records are maintained in the Verification Information System (VIS) at the USCIS Headquarters in Washington, DC and field offices.

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 information; employers who 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; USCIS employees and contractors who have access to E-Verify for operation, maintenance, monitoring, and compliance purposes including, USCIS status verifiers, managers, and administrators; and individuals who may have been victims of identity theft and have chosen to lock their SSN from further use in the E-Verify program.

CATEGORIES OF RECORDS IN THE SYSTEM:

Employment eligibility information entered into E-Verify by the E-Verify employer about the employee to be verified.

- All Employees:
  - Name (last, first, middle initial, maiden);
  - Date of Birth;
  - Social Security Number;
  - Date of Hire;
  - Three day hire date expiration:
    - Awaiting SSN;
    - Technical Problems;
    - Audit Revealed New Hire Was Not Run;
    - Federal Contractor With E-Verify Clause Verifying Existing Employees; and
    - Other.
  - Claimed Citizenship Status;
  - Type of identity document presented by employee to the employer during Form I–9 preparation process;
  - Expiration Date of identity document presented by employee to the employer during Form I–9 preparation process;
  - State or jurisdiction of issuance of identity document presented by the employee to the employer during the Form I–9 process when that document is a driver's license, driver's permit, or state-issued identification (ID) card;
  - Document number of identity document presented by the employee to the employer during the Form I–9 preparation process when that document is a driver's license, driver's permit, or state-issued ID issued by a state or jurisdiction participating in the Records and Information from Departments of Motor Vehicles for E-Verify (RIDE) program and where an Memorandum of Agreement (MOA) exists between the state or jurisdiction and DHS USCIS to verify the information about the document;
  - Photographs, if required by secondary verification;
  - Disposition data from the employer. The following descriptors are entered by the employer based on the action taken by the employer as a result of the employment verification information:
    - The employee continues to work for the employer after receiving and Employment Authorized (EA) result: employer selects this option based on receiving an EA 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 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 of 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.
- Non-U.S. Citizens:
  - A–Number; and
  - I–94 Number.
- Information about the 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
- E–Mail Address.

• 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;
- E-mail Address; and
- User ID.

• Employment Eligibility Information created by E-Verify:

- Case Verification Number;
- VIS Response:
- Employment Authorized;
- SSA TNC;
- DHS TNC;
- 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 Verification in Process;
- DHS Employment Unauthorized;
- DHS No Show; and
- DHS FNC.
- Monitoring and Compliance Information created as part of E-Verify: The Verification Division monitors E-Verify to minimize and prevent misuse and fraud of the system. This monitoring information, and the accompanying compliance information, may in some cases be placed in the electronic or paper files that make up E-Verify.) The information may include:

- Analytic or other information derived from monitoring;
- Compliance activities, including information placed in the Compliance Tracking and Management System (CTMS);
- Complaint or hotline reports;
- Records of communication;
- Other employment and E-Verify related records, documents, or reports derived from compliance activities, especially in connection with determining the existence of fraud or discrimination in connection with the use of the E-Verify system; and
- Information derived from telephone calls, e-mails, letters, desk audits or site visits, as well as information from media reports or tips from law enforcement agencies.

• Information collected from Motor Vehicle Agencies (MVAs) and used to verify of the information from a driver's license, permit, or state issued ID card when those documents are presented as documents to establish identity by an employee to an employer during the E-Verify process, and when the jurisdiction under which the document was issued has established a MOA with DHS USCIS to allow verification of this information. Additional manual verification may be required if E-Verify is unable to verify the information submitted by the employer during the automated process. While each state MVA may collect different types of information, information provided to E-Verify may include the following:

- Last Name;
- First Name;
- State or Jurisdiction of Issuance;
- Document Type;
- Document Number;
- Date of Birth;
- Status Text;
- Status Description Text; and
- Expiration Date.
- Information used to verify employment eligibility. (E-Verify uses VIS as the transactional database to verify the information provided by the employee. VIS contains the E-Verify transaction information. If E-Verify is unable to verify employment eligibility through VIS, additional manual verification may be required. These automated and manual verifications may include the following databases.)
- Social Security Administration Numident System;
- USCIS Central Index System (CIS);
- CBP Nonimmigrant Information System (NIIS) and Border Crossing Information (BCI);
- USCIS Computer-Linked Application Information Management System Version 3 (CLAIMS 3);
- USCIS Computer-Linked Application Information Management System Version 4 (CLAIMS 4);
- USCIS Image Storage and Retrieval System (ISRS);
- ICE Student and Exchange Visitor Identification System (SEVIS);
- USCIS Reengineered Naturalization Applications Casework System (RNACS);
- USCIS Aliens Change of Address System (AR–11);
- USCIS National File Tracking System (NFTS);
- USCIS Microfilm Digitization Application System (MiDAS);
- USCIS Marriage Fraud Amendment System (MFAS);
- USCIS Citizenship and Immigration Services Centralized Operational Repository (CISCOR);
- Department of State Consular Consolidated Database (CCD);
- USCIS Enterprise Document Management System (EDMS);
- ICE ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM) Alien Number;
- USCIS Refugees, Asylum, and Parole System (RAPS);
- US–VISIT Arrival Departure Information System (ADIS); and
- Department of Justice Executive Office Immigration Review System (EOIR).

• These databases may contain some or all of the following information which will be incorporated into the E-Verify SORN as part of this verification process:

- Last Name;
- First Name;
- Middle Name;
- Maiden Name;
- Date of Birth;
- Age;
- Country of Birth;
- Country of Citizenship;
- Alien Number;
- Social Security Number;
- 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; and
- 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;
- 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); and
- Federal Bureau of Investigation Number;
- Admission Number; and
- Petitioner Firm Name;
- Petitioner Tax Number;
- Date of Admission;
- Marital Status;
- Marriage Date and Place;
- Marriage Information and Certificate;
- Visa Control Number;
- FOIL Number;
- Class of Admission;
- Federal Bureau of Investigation Number;
- 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;
- File Location; and
- Decision memoranda, investigatory reports and materials compiled for the purpose of enforcing immigration laws, exhibits, transcripts, and other case-related papers concerning aliens, alleged aliens or lawful permanent residents brought into the administrative adjudication process.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104–208, dated September 30, 1996.

PURPOSE(S):

This system provides employment authorization information to employers participating in E-Verify. 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 registrations by employers;
- Inappropriate registration 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 as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

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

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 where DOJ or DHS has agreed to represent the employee; or

4. The United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

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 or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency, organization, or individual 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. The Department 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, where 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 from 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 Records and Information from Departments of Motor Vehicles for E-Verify (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 it is determined 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, 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:

The retention and disposal schedule, N1–566–08–7 is approved by the National Archives and Records Administration. Records collected in the process of enrolling in E-Verify and in verifying employment eligibility are stored and retained in E-Verify for ten (10) years, from the date of the completion of the last transaction unless the records are part of an on-going 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, U.S. Citizenship and Immigration Services, 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 Verification Division FOIA Officer, whose contact information can be found at *http://www.dhs.gov/foia* under "contacts." 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, 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. 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 provide the following:

- An explanation of 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;
- Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records; and
- 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 this bulleted 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 as listed in the Category of Records section above; and (D) Information created by E-Verify, including its monitoring and compliance activities.

EXEMPTIONS CLAIMED FOR THE SYSTEM:

None.

Dated: April 25, 2011.

Mary Ellen Callahan,

Chief Privacy Officer, Department of Homeland Security.

[FR Doc. 2011–11291 Filed 5–6–11; 8:45 am]

BILLING CODE P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[USCG–2011–0336]

Information Collection Requests to Office of Management and Budget; OMB Control Numbers: 1625–0077, 1625–0085 and 1625–0112

AGENCY: Coast Guard, DHS.

ACTION: Sixty-day notice requesting comments.

SUMMARY: In compliance with the Paperwork Reduction Act of 1995, the U.S. Coast Guard intends to submit Information Collection Requests (ICRs) to the Office of Management and Budget (OMB), Office of Information and Regulatory Affairs (OIRA), requesting an extension of its approval for the following collections of information: 1625–0077, Security Plans for Ports, Vessels, Facilities, and Outer Continental Shelf Facilities and Other Security-Related Requirements; 1625–0085, Streamlined Inspection Program; and 1625–0112, Enhanced Maritime Domain Awareness via Electronic Transmission of Vessel Transit Data. Our ICRs describe the information we seek to collect from the public. Before submitting these ICRs to OIRA, the Coast Guard is inviting comments as described below.

DATES: Comments must reach the Coast Guard on or before July 8, 2011.

ADDRESSES: You may submit comments identified by Coast Guard docket number [USCG–2011–0336] to the Docket Management Facility (DMF) at the U.S. Department of Transportation (DOT). To avoid duplicate submissions, please use only one of the following means:

(1) *Online: http://www.regulations.gov.*

(2) *Mail:* DMF (M–30), DOT, West Building Ground Floor, Room W12–140, 1200 New Jersey Avenue, SE., Washington, DC 20590–0001.

(3) *Hand delivery:* Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202–366–9329.

(4) *Fax:* 202–493–2251. To ensure your comments are received in a timely manner, mark the fax, to attention Desk Officer for the Coast Guard.

The DMF maintains the public docket for this Notice. Comments and material received from the public, as well as documents mentioned in this Notice as being available in the docket, will become part of the docket and will be available for inspection or copying at room W12–140 on the West Building Ground Floor, 1200 New Jersey Avenue, SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find the docket on the Internet at *http://www.regulations.gov*.

Copies of the ICRs are available through the docket on the Internet at *http://www.regulations.gov*. Additionally, copies are available from: COMMANDANT (CG–611), ATTN PAPERWORK REDUCTION ACT MANAGER, U.S. COAST GUARD, 2100 2ND ST., SW., STOP 7101, WASHINGTON, DC 20593–7101.

FOR FURTHER INFORMATION CONTACT: Contact Ms. Kenlinishia Tyler, Office of Information Management, telephone 202–475–3652, or fax 202–475–3929, for questions on these documents. Contact Ms. Renee V. Wright, Program Manager, Docket Operations, 202–366–9826, for questions on the docket.

SUPPLEMENTARY INFORMATION:

Public Participation and Request for Comments

This Notice relies on the authority of the Paperwork Reduction Act of 1995; 44 U.S.C. chapter 35, as amended. An ICR is an application to OIRA seeking the approval, extension, or renewal of a Coast Guard collection of information (Collection). The ICR contains information describing the Collection's purpose, the Collection's likely burden on the affected public, an explanation of the necessity of the Collection, and other important information describing the Collections. There is one ICR for each Collection.

The Coast Guard invites comments on whether these ICRs should be granted based on the Collections being necessary for the proper performance of Departmental functions. In particular, the Coast Guard would appreciate comments addressing: (1) The practical utility of the Collections; (2) the accuracy of the estimated burden of the Collections; (3) ways to enhance the quality, utility, and clarity of information subject to the Collections; and (4) ways to minimize the burden of the Collections on respondents, including the use of automated collection techniques or other forms of information technology. In response to your comments, we may revise these ICRs or decide not to seek approval for the Collections. We will consider all comments and material received during the comment period.

We encourage you to respond to this request by submitting comments and related materials. Comments must contain the OMB Control Number of the ICR and the docket number of this request, [USCG–2011–0336], and must be received by July 8, 2011. We will post all comments received, without change, to *http://www.regulations.gov*. They will include any personal information you provide. We have an agreement with DOT to use their DMF. Please see the "Privacy Act" paragraph below.

Submitting Comments

If you submit a comment, please include the docket number [USCG–2011–0336], indicate the specific section of the document to which each comment applies, providing a reason for each comment. You may submit your comments and material online (*via http://www.regulations.gov*), by fax, mail, or hand delivery, but please use only one of these means. If you submit a comment online via *http://www.regulations.gov,* it will be considered received by the Coast Guard when you successfully transmit the comment. If you fax, hand deliver, or mail your comment, it will be considered as having been received by the Coast Guard when it is received at the DMF. We recommend you include your name, mailing address, an e-mail address, or other contact information in the body of your document so that we can contact you if we have questions regarding your submission.

You may submit your comments and material by electronic means, mail, fax, or delivery to the DMF at the address under **ADDRESSES**; but please submit them by only one means. To submit your comment online, go to *http://www.regulations.gov,* and type "USCG–2011–0336" in the "Keyword" box. If you submit your comments by mail or hand delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit comments by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during the comment period and will address them accordingly.

Viewing comments and documents: To view comments, as well as documents mentioned in this Notice as being available in the docket, go to