[Federal Register: May 19, 2010 (Volume 75, Number 96)]
[Notices]
[Page 28035-28042]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
[DOCID:fr19my10-78]

DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

[Docket No. DHS-2010-0038]

Privacy Act of 1974; Department of Homeland Security/U.S. Citizenship and Immigration Services--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 establish a new Department of Homeland Security system of records notice 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 check citizenship status and verify employment eligibility of newly hired employees. Previously, these records were covered under Department of Homeland Security/U.S. Citizenship and Immigration Services--004 Verification Information System of Records, December 11, 2008, along with records from the U.S. Citizenship and Immigration Services Systematic Alien Verification for Entitlements (SAVE) Program. In order to provide clearer transparency and enable public understanding, the Department is publishing two separate systems of records for U.S. Citizenship and Immigration Services E-Verify and SAVE Programs. This newly established system will be included in the Department of Homeland Security's inventory of record systems. The U.S. Citizenship and Immigration Services SAVE Program system of records notice can be found elsewhere in the Federal Register.

DATES: Submit comments on or before June 18, 2010. This new system will be effective June 18, 2010.

ADDRESSES: You may submit comments, identified by docket number DHS-2010-0038 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: Claire Stapleton, Privacy Branch Chief, Verification Division, U.S. Citizenship and Immigration Services, Department of Homeland Security, Washington, DC 20529. 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) U.S. Citizenship and Immigration Services (USCIS) proposes to establish a new

[[Page 28036]]

DHS system of records titled, ``DHS/USCIS--011 E-Verify Program System of Records.''

E-Verify was 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 I-9 (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.

Previously, USCIS addressed E-Verify Program and the Systematic Alien Verification for Entitlements (SAVE) Program in the same Privacy Impact Assessment (PIA) and System of Records Notice (SORN) titled, DHS/USCIS--004 Verification Information System (VIS) of Records, December 11, 2008. VIS was and continues to be the underlying technology of both systems. This SORN, which describes E-Verify independently from SAVE, is written to provide clearer transparency and enable public understanding of these programs. USCIS has prepared a separate SORN to discuss the SAVE Program and can be found elsewhere in the Federal Register.

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. For example, some states require that all employers must use E-Verify, while other states require that all state job services must use E-

Verify. Additionally, the federal government requires E-Verify checks for all government employees and federal contractors.

E-Verify is a fully operational web based program that allows any employer to enroll and begin to verify employees' employment eligibility. The following describes the complete E-Verify process.

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. 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 designated 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 designated agent, can then create user accounts for the employees who will 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, Social Security Number (SSN), and information from the documents provided on Form I-9, into the E-Verify online user interface tool. Form I-9 has 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 U.S. are required to use this form regardless of whether they are enrolled in E-Verify.
Processing Non-United States Citizens

For non-USCs, including immigrants, non-immigrants, and lawful permanent residents, the vast majority of queries are completed when E-Verify verifies the name, SSN, and birth date against SSA's Numident system, followed by the name, date of birth, and Form I-9 document information against certain DHS databases. The specific DHS 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 A-Number will be 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 Form I-94 number against the CBP Non Immigrant Information System (NIIS) and Border Crossing Information System (BCI). If both SSA and DHS are able to verify the employee`s employment eligibility the employer receives an Employment Authorized notification. E-Verify generates a case verification number and the employer may either print and retain the Case Details page

[[Page 28037]]

from E-Verify or write the case verification number on Form I-9.

If the automated query does not immediately result in an Employment Authorized 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 with information in DHS 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 will receive the Employment Authorized notification.

If the USCIS Status Verifiers are unable to confirm employment eligibility, E-Verify will display a DHS Tentative Non-Confirmation (TNC) response and generate a TNC Notice for the employer to print and give to the employee, which explains that the employee has received a TNC without going into detail as to specifically what caused the TNC. The letter also explains the employee's rights, and gives him the opportunity to decide if he will contest the result with DHS. If the employee wishes to contest the TNC, the employee must notify his employer, who indicates so in E-Verify and DHS E-Verify generates a Referral Letter. This letter instructs the employee that he has 8 days to contact USCIS Status Verifiers to resolve the discrepancy. Once the employee contacts the USCIS Status Verifiers, the USCIS Status

Verifiers will 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 databases to determine whether there is any other information pertaining to that individual that would confirm the employment eligibility status. To conduct these databases searches, USCIS Status Verifiers may use a Person Centric Query System to facilitate the information search. If the USCIS Status Verifier determines that the employee is eligible to work, the USCIS Status Verifier will indicate this in E-Verify, which will then notify the employer that the employee is Employment Authorized. If the Status Verifier determines that an employee is not eligible to work, the Status Verifier will update E-Verify with an Final Non-Confirmation (FNC) disposition and E-Verify will notify 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 the action taken. If an employer retains an employee who has received final confirmation that he is not eligible to work, and fails to notify DHS, the employer may be liable for failure to notify and knowingly employing an individual who is not eligible to work.

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 (USC) who used a U.S. passport for completing Form I-9, the E-Verify tool will present to the employer the photo on record for the applicable document. The DHS photos come from DHS's ISRS database, and the passport photos come from a copy of the Department of State passport data contained in TECS. This feature is known as the Photo Screening Tool. The employer will visually compare 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 Employment Authorized 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 that there is a mismatch that results in a TNC, the employee will be notified that they need to provide a photocopy of their document to a USCIS Status Verifier. The USCIS Status Verifier will do various searches to try to confirm the information supplied by the employee. In cases where the information cannot be matched because the employee is asserting that there is a mistake in the document, the employee will be sent to the USCIS Application Support Center for resolution. E-Verify requires that employers photocopy and retain a copy of the employee's Form I-9 documentation if it is Form I-766 or I-551.

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 an employee has been hired. Further, the employer must perform E-Verify queries for newly hired employees no later than the third (3rd) 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, 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 or from its monitoring and compliance activities or call center contacts, including but not limited to records of interviews, employment and E-Verify-related documents and other records obtained in the course of carrying out its monitoring and compliance activities, especially in connection with determining the existence of fraud or discrimination in connection with the use of the E-Verify system. Data generated from this effort is stored in the CTMS system; (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; and (5) Activities in support of law enforcement to prevent fraud and misuse of E-Verify, and to prevent discrimination and identity theft.

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 United States 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 that are 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

DHS/USCIS--011

System name:

DHS/USCIS--011 E-Verify Program System of Records.

Security classification:

Unclassified, for official use only.

System location:

Records are maintained at the USCIS Headquarters in Washington, D.C. and field offices.

Categories of individuals covered by the system:

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 social security number from further use in the E-Verify program.

Categories of records in the system:

Employment eligibility information collected from the E-Verify employer about the employee to be verified.

All Employees:

[cir] Name (last, first, middle initial, maiden);
[cir] Date of Birth;
[cir] Social Security Number;
[cir] Date of Hire;
[cir] Three day hire date expiration:
[dec222] Awaiting SSN;
[dec222] Technical Problems;
[dec222] Audit Revealed New Hire Was Not Run;
[dec222] Federal Contractor With E-Verify Clause Verifying Existing Employees; and
[dec222] Other.
[cir] Claimed Citizenship Status;
[cir] Type of Document Used for Acceptable Form I-9 Verification;
[cir] Acceptable Form I-9 Document Expiration Date;

[cir] Photographs, if required by secondary verification;

[cir] 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:

[dec222] The employee continues to work for the employer after receiving and Employment Authorized result: Employer selects this option based on receiving an Employment Authorized response from E-Verify;

[dec222] The employee continues to work for the employer after receiving a Final Nonconfirmation result: Employer selects this option based on the employee getting an FNC despite the employee contesting the TNC and the employer retains the employee;

[dec222] 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 SSA or DHS and the employer retains the employee;

[dec222] The employee continues to work for the employer after choosing not to contest a Tentative Nonconfirmation: Employer selects this option when the employee does not contest the TNC but the employer retains the employee;

[dec222] The employee was terminated by the employer for receiving a Final Nonconfirmation result: Employer selects this option when employee receives FNC and is terminated;

[dec222] 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;

[dec222] The employee was terminated by the employer for choosing not to contest a Tentative Nonconfirmationt: Employer selects this option when employee does not contest the TNC and is terminated;

[dec222] The employee voluntarily quit working for the employer: Employer selects this option when employee voluntarily quits job without regard to E-Verify;

[dec222] 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;

[dec222] 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

[dec222] 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-USCs:

[cir] A-Number; and

[cir] I-94 Number.

Information about the Employer or Designated Agent:

[cir] Company Name;

[cir] Street Address;

[cir] Employer Identification Number;

[cir] North American Industry Classification System (NAICS) Code;

[cir] Number of Employees;

[cir] Number of Sites;

[cir] Parent Company or Corporate Company;

[cir] Name of Company Point of Contact;

[cir] Phone Number;
[cir] Fax Number;
[cir] E-Mail Address.

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

[cir] Last Name;
[cir] First Name;
[cir] Middle Initial;
[cir] Phone Number;
[cir] Fax Number;
[cir] E-mail Address; and
[cir] User ID.

Employment Eligibility Information created by E-Verify:

[cir] Case Verification Number;
[cir] VIS Response:
[dec222] Employment Authorized;
[dec222] SSA TNC;
[dec222] DHS TNC;
[dec222] SSA Case in Continuance (In rare cases SSA needs more than 10 federal government workdays to confirm employment eligibility);
[dec222] DHS Case in Continuance (In rare cases DHS needs more than 10 federal government workdays to confirm employment eligibility);
[dec222] SSA FNC;
[dec222] DHS Verification in Process;
[dec222] DHS Employment Unauthorized;
[dec222] DHS No Show; and
[dec222] DHS FNC.

Monitoring and Compliance Information created as part of E-Verify (USCIS 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:

[cir] Analytic or other information derived from monitoring and compliance activities, including information placed in CTMS;
[cir] Complaint or hotline reports;
[cir] Records of communication;
[cir] 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
[cir] 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 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 other DHS databases.)

Social Security Administration Numident System:

[cir] Confirmation of Employment Eligibility;
[cir] TNC of Employment Eligibility and Justification; and
[cir] FNC of Employment Eligibility.

USCIS Central Index System:

[cir] Alien Number;
[cir] Last Name;

[cir] First Name;
[cir] Middle Name;
[cir] Date of Birth;
[cir] Date Entered United States;
[cir] Country of Birth;
[cir] Class of Admission;
[cir] File Control Office Code;
[cir] Social Security Number;
[cir] Form I-94 Number;
[cir] Provision of Law Cited for Employment Authorization;
[cir] Office Code Where the Authorization Was Granted;
[cir] Date Employment Authorization Decision Issued;
[cir] Date Employment Authorization Begins;
[cir] Date Employment Authorization Expires;
[cir] Date Employment Authorization Denied;
[cir] Naturalization Certificate Number; and
[cir] EOIR Information, if in Proceedings.

CBP Nonimmigrant Information System (NIIS) and Border Crossing Information (BCI):

[cir] Alien Number;
[cir] Last Name;
[cir] First Name;
[cir] Maiden Name;
[cir] Date Alien's Status Changed;
[cir] Date of Birth;
[cir] Class of Admission Code;
[cir] Date Admitted Until;
[cir] Country of Citizenship;
[cir] Port of Entry;
[cir] Date Entered United States;
[cir] Departure Date;
[cir] I-94 Number;
[cir] Visa Number;
[cir] Passport Number;
[cir] Passport Information; and
[cir] Passport Card Number.

USCIS Image Storage and Retrieval System (ISRS):

[cir] Receipt Number;
[cir] Alien Number;
[cir] Last Name;
[cir] First Name;
[cir] Middle Name;
[cir] Date of Birth;
[cir] Country of Birth;
[cir] Form Number, for example Form I-551 (Lawful Permanent Resident card) or Form I-766 (Employment Authorization Document);
[cir] Expiration Date; and
[cir] Photograph.

USCIS Computer-Linked Application Information Management System Version 3 (CLAIMS 3):

[cir] Receipt Number;
[cir] Alien Number;
[cir] Last Name;
[cir] First Name;
[cir] Middle Name;
[cir] Address;
[cir] Social Security Number;

[cir] Date of Birth;
[cir] Country of Birth;
[cir] Class of Admission;
[cir] I-94 Number;
[cir] Employment Authorization Card Information;
[cir] Lawful Permanent Resident Card Information;
[cir] Date of Entry;
[cir] Valid To Date;
[cir] Petitioner Internal Revenue Service Number;
[cir] Attorney Name; and
[cir] Attorney Address.

ICE Student and Exchange Visitor Identification System (SEVIS):

[cir] Student and Exchange Visitor Identification Number;
[cir] Last Name;
[cir] First Name;
[cir] Middle Name;
[cir] Date of Birth;
[cir] Country of Birth;
[cir] Class of Admission;
[cir] I-94 Number;
[cir] Date of Entry;
[cir] Valid To Date;
[cir] Social Security Number;
[cir] Nationality;
[cir] Gender;
[cir] Student Status;
[cir] Visa Code;
[cir] Status Change Date;
[cir] Port of Entry Code;
[cir] Non Citizen Entry Date;
[cir] Status Code; and
[cir] Program End Date.

USCIS Computer-Linked Application Information Management System Version 4 (CLAIMS 4):

[cir] Alien Number;
[cir] Social Security Number;
[cir] Last Name;
[cir] First Name;
[cir] Middle Name;
[cir] Birth Date;
[cir] Birth Country;
[cir] Nationality;
[cir] Gender;

[[Page 28040]]

[cir] Naturalization Verification (Citizenship Certificate Identification ID);
[cir] Naturalization Verification (Citizenship Naturalization Date/Time); and
[cir] Address.

USCIS Reengineered Naturalization Applications Casework System (RNACS):

[cir] Alien Number;
[cir] Last Name;
[cir] First Name;

[cir] Middle Name;
[cir] Birth Date;
[cir] Birth Country;
[cir] Gender;
[cir] Nationality;
[cir] Naturalization Verification (Citizenship Naturalization Date/Time);
[cir] Naturalization Verification (Citizenship Certificate Identification ID);
[cir] Immigration Status (Immigration Status Code); and
[cir] Address.

USCIS Aliens Change of Address System (AR-11):

[cir] Name;
[cir] Current Address;
[cir] Date of Birth;
[cir] Previous Address;
[cir] Alien Number;
[cir] Federal Bureau of Investigation Number;
[cir] Admission Number; and
[cir] Previous Address.

USCIS Citizenship and Immigration Services Centralized Operational Repository (CISCOR):

[cir] Receipt Number;
[cir] Beneficiary Alien Number;
[cir] Beneficiary Date of Birth;
[cir] Beneficiary Country of Birth;
[cir] Beneficiary Social Security Number;
[cir] Beneficiary Last Name;
[cir] Beneficiary First Name;
[cir] Beneficiary Middle Name;
[cir] Petitioner Alien Number;
[cir] Petitioner Social Security Number;
[cir] Petitioner Naturalization Certificate Number;
[cir] Petitioner First Name;
[cir] Petitioner Last Name;
[cir] Petitioner Firm Name; and
[cir] Petitioner Tax Number.

USCIS National File Tracking System (NFTS):

[cir] Alien Number; and
[cir] File Location.

USCIS Microfilm Digitization Application System (MiDAS):

[cir] Name;
[cir] Alien Number;
[cir] Date of Birth; and
[cir] Citizenship Number.

USCIS Marriage Fraud Amendment System (MFAS):

[cir] Individual:
[dec221] Name (Last, First, Middle);
[dec221] Date of Birth;
[dec221] Country of Birth;
[dec221] Country of Citizenship;
[dec221] Class of Admission;
[dec221] Date of Admission;
[dec221] Alien Number;
[dec221] Receipt Number;
[dec221] Phone Number; and
[dec221] Marriage Date and Place.

[cir] Spouse:
[dec221] Name (Last, First, Middle);
[dec221] Date of Birth;
[dec221] Country of Birth;
[dec221] Country of Citizenship;
[dec221] Class of Admission;
[dec221] Date of Admission;
[dec221] Alien Number;
[dec221] Receipt Number;
[dec221] Phone Number;
[dec221] Marriage Date and Place; and
[dec221] Naturalization Date and Place.
[cir] Children:
[dec221] Names (Last, First, Middle);
[dec221] Date of Birth;
[dec221] Country of Birth;
[dec221] Class of Admission; and
[dec221] Alien Number.
[cir] Employer:
[dec221] Name;
[dec221] Address;
[dec221] Supervisor's Name; and
[dec221] Supervisor's Phone Number.
USCIS Enterprise Document Management System (EDMS):
[cir] All information contained in an individual's A-File, including, but not limited to:
[dec221] Alien Number;
[dec221] Last Name;
[dec221] First Name;
[dec221] Middle Name;
[dec221] Date of Birth;
[dec221] Date Entered United States;
[dec221] Country of Birth;
[dec221] Class of Admission;
[dec221] Social Security Number;
[dec221] Form I-94 Number;
[dec221] Naturalization Information and Certificate;
[dec221] Photograph; and
[dec221] Marriage Information and Certificate.
Department of State Consular Consolidated Database (CCD):
[cir] Name;
[cir] Date of Birth;
[cir] Passport Number;
[cir] Visa Control Number;
[cir] FOIL Number;
[cir] Alien Number; and
[cir] Photograph.
ICE ENFORCE Integrated Database (EID) Enforcement Alien Removal Module (EARM) Alien Number:
[cir] Name;
[cir] Marital Status;
[cir] Date of Birth;
[cir] Age;
[cir] Sex;
[cir] Country of Birth;
[cir] Country of Citizenship;
[cir] Date of Entry;

[cir] Class of Admission;
[cir] Social Security Number;
[cir] Federal Bureau of Investigation Number;
[cir] Case History;
[cir] Alerts;
[cir] Case Summary Comments;
[cir] Case Category;

[cir] Date of Encounter;
[cir] Encounter Information;
[cir] Custody Actions & Decisions;
[cir] Case Actions & Decisions;
[cir] Bonds; and
[cir] Photograph.

USCIS Refugees, Asylum, and Parole System (RAPS):

[cir] Class of Admission;
[cir] Country of Birth;
[cir] Date of Birth;
[cir] Date of Entry;
[cir] Current Status; and
[cir] Asylum Applicant Receipt Date.

US-VISIT Arrival Departure Information System (ADIS):

[cir] Last Name;
[cir] First Name;
[cir] Date of Birth;
[cir] Country of Citizenship;
[cir] Sex;
[cir] Passport Number;
[cir] Airline and Flight Number;
[cir] Country of Residence;
[cir] City Where Boarded;
[cir] City Where Visa was Issued;
[cir] Date Visa Issued;
[cir] Address While in United States; and
[cir] Port of Entry.

Department of Justice Executive Office Immigration Review System (EOIR):

[cir] Name;
[cir] File Number;
[cir] Address;
[cir] Nationality; and
[cir] 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):

The purpose of this system is to provide 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, 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 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.

J. 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 number, Alien Number, I-94 Number, Receipt Number, Passport (U.S. or Foreign) Number, or Social Security Number 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, has been 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 20529.

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 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.

Mary Ellen Callahan,
Chief Privacy Officer, Department of Homeland Security.
[FR Doc. 2010-11972 Filed 5-18-10; 8:45 am]
BILLING CODE 9111-97-P