Privacy Impact Assessment
for the

# E-Verify Program

May 4, 2010


**Contact Point**
**Claire Stapleton**
**Privacy Branch Chief**
**Verification Division**
**United States Citizenship and Immigration Services**

**Reviewing Official**
**Donald Hawkins**
**Chief Privacy Officer**
**United States Citizenship and Immigration Services**
**(202) 272-8000**

**Mary Ellen Callahan**
**Chief Privacy Officer**
**Department of Homeland Security**
**(703) 235-0780**

## Abstract

The Verification Division of the U.S. Citizenship and Immigration Services (USCIS) provides a service that allows employers to verify the employment eligibility of their newly hired employees through an electronic verification program called E-Verify. Previously, USCIS addressed the E-Verify program as part of the Verification Information System (VIS) PIA. USCIS is conducting a separate PIA for E-Verify in order to better assist the public in understanding this program.

## Overview

E-Verify is a free, and in most cases voluntary, Department of Homeland Security (DHS) program implemented by the United States Citizenship and Immigration Services (USCIS) and operated in collaboration with the Social Security Administration (SSA). It allows employers to compare information provided by employees on the *Employment Eligibility Verification*, Form I-9, against information in SSA and DHS databases in order to verify that an employee is authorized to work in the U.S., either because he is a U.S. citizen or is a non-citizen whom the United States has granted work authorization.[1] E-Verify was mandated by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA).[2]

Previously, DHS had published a single Privacy Impact Assessment (PIA) and System Of Records Notice (SORN) for both E-Verify and the Systematic Alien Verification for Entitlements (SAVE) Programs as part of the underlying technology, the Verification Information System (VIS). In addition, DHS has published a PIA for the Person Centric Query System (PCQS) which supported both SAVE and E-Verify. DHS is now publishing separate PIAs for E-Verify and SAVE in order to assist the public in understanding these programs and incorporating appropriate information from both VIS and PCQS PIAs. In addition, E-Verify is making a change to the processing of certain E-Verify verification requests involving employees who provide their U.S. passports for the Form I-9 documentation. Upon publication of the E-Verify and SAVE PIAs the VIS PIAs will be retired, but the PCQS PIAs will remain because they provide a more detailed explanation of the service as part of the overall USCIS service oriented architecture.[3] USCIS has prepared a separate PIA to discuss SAVE.

---

[1] All U.S. employers are responsible for the completion and retention of Form I-9 for each individual they hire for employment in the United States including citizens and non-citizens. On the form, the employer must verify the employment eligibility and identity documents presented by the employee and record certain identity document information on Form I-9.

[2] The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law (P.L.) 104-208, September 30, 1996. Originally designated as the "Basic Pilot" program.

[3] USCIS Person Centric Query Service Supporting the Verification Division Information System Update, January 18, 2008; USCIS Person Centric Query Service Supporting Immigration Status Verifiers of the USCIS National Security and Records Verification Directorate/Verification Division Update, January18, 2008; and USCIS Person Centric Query

A companion monitoring and compliance program, the Compliance and Tracking Management System (CTMS) supports E-Verify. CTMS allows DHS to identify unlawful or impermissible uses of E-Verify. Any improper use of the system may be referred to ICE or the Department of Justice (DOJ) for additional investigation or prosecution. CTMS is more fully described in the CTMS SORN and PIA.[4]

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 responsibilities and USCIS was charged with operating the Basic Pilot Program. In addition to changing the name from the Basic Pilot Program to the E-Verify Program, USCIS has continued to develop the program as the requirements for employment verification have changed. Although the government only mandates the use of E-Verify in limited cases, such as for federal government employees, employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation E-Verify clause, some states require that all employers use E-Verify, while other states require that all state job services use E-Verify.

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 E-Verify process from beginning to end.

**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 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[5]

---

Service Supporting Immigration Status Verifiers of the USCIS National Security and Records Verification Directorate/Verification Division Update, August 13, 2008 can be found on the DHS Privacy website, www.dhs.gov/privacy.

[4] 74 FR 33825, Compliance Tracking and Monitoring System (CTMS) SORN, May 22, 2009; the CTMS PIA dated May 22, 2009 can be found on the DHS Privacy website, www.dhs.gov/privacy.

[5] The NAICS is the standard used by Federal statistical agencies in classifying business establishments for the purpose

- 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
- POC E-Mail Address

Participants, whether an employer or designated agent, can than 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
- User ID

---

of collecting, analyzing, and publishing statistical data related to the U.S. business economy.

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, which includes submitting the electronically signed MOU to E-Verify, E-Verify emails a unique user login and password to every user that has been created as described above. E-Verify instructs the users to take the online E-Verify proficiency tutorial. All users must pass the mastery test at the end of the tutorial before they can use E-Verify to verify employment eligibility. 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. The posters are in both English and Spanish. Once the employer has placed the E-Verify posters for display and users have passed the mastery test, they may begin using E-Verify.

**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 for the Form I-9, into the E-Verify online user interface tool.[6] Employers already collect most and sometimes all of the information required for E-Verify, in Sections 1 and 2 of Form I-9. The Form I-9 has a field for the SSN but the employee is not required to provide this number on the form unless the employer is a 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 the SSA's Numident[7], followed by the name, birth date, 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 Central Index System (CIS), and the EAD photograph, as described below against the Image Storage and Retrieval System (ISRS). If the employee is a non-immigrant, E-Verify queries the Form I-94 number against Nonimmigrant Information System (NIIS)[8] and Border Crossing Information[9] over the TECS. 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

[6] Pursuant to the Federal Acquisition Rule (FAR), government contractors must verify employees under the certain government contracts to ascertain employment eligibility for new and existing employees.
[7] 71 FR 1796, SORN for the SSA NUMIDENT System.
[8] 73 FR 77739 DHS/CBP-016 – Nonimmigrant Information System
[9] 73 FR 43457 DHS/CBP-007 Border Crossing Information (BCI)

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 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 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. 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 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 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 E-Verify Status Verifiers to resolve the discrepancy in their record. Once the employee contacts the Status Verifiers, the 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.[10] To conduct these databases searches, Status Verifiers may use PCQS to facilitate the information search. If the Status Verifier determines that the employee is eligible to work, the 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 FNC disposition and E-Verify will notify the employer of this

[10] E-Verify may conduct verifications against the following Federal government systems; SSA's Numident, USCIS's Central Index System (CIS), Image Storage and Retrieval System (ISRS), Computer-Linked Application Information Management System Version 3 (CLAIMS 3), Computer-Linked Application Information Management System Version 4.0 (CLAIMS 4), Reengineered Naturalization Applications Casework System (RNACS), Aliens Change of Address System (AR-11) , Citizenship and Immigration Services Centralized Operational Repository (CISCOR), National File Tracking System (NFTS), Microfilm Digitization Application System (MiDAS), Refugees, Asylum, and Parole System (RAPS), Marriage Fraud Amendment System (MFAS), Department of Justice's (DOJ)'s Executive Office Immigration Review System (EOIR), Department of State (DOS)'s Consular Consolidated Database (DOS-CCD), Immigration and Custom Enforcement (ICE)'s Student and Exchange Visitor Identification System (SEVIS), ENFORCE Integrated Database (EID), Customs and Border Protection(CBP)'s TECS, and United State Visitor and Immigrant Status Indicator Technology (US-VISIT)'s Arrival Departure Information System (ADIS). The applicable SORNs for these systems are included in Section 2 of the PIA. The specific data elements verified are described below in Section 1 of this PIA.

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 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 DHS and providing additional information. If the employer reports that there is a mismatch that results in an FNC, the employee will be notified that they need to provide a photocopy of their document to the Status Verifiers. The status verifiers will do various searches to try to confirm, in cases where the information cannot be matched because the employee is asserting that there is a mistake in the document, they 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. For example, it minimizes pre-screening employees, which the employer could then use as an excuse to not hire a particular individual.

While E-Verify primarily uses the information it collects for verification of employment eligibility, the information may also be used to prevent fraud and misuse of E-Verify, and to

prevent discrimination and employment-based 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 related to the use of E-Verify. The Verification Division uses information contained in E-Verify for several purposes, including:

- Program management, which may include documentary repositories of business information, internal and external audits, congressional requests, and program reports.
- 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. A call center may make outgoing or receive incoming calls regarding E-Verify. This includes using information for testing purposes.
- 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.
- 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.
- Activities in support of law enforcement to prevent fraud and misuse of E-Verify, and to prevent discrimination and identity theft.

# Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

## 1.1 What information is collected, used, disseminated, or maintained in the system?

E-Verify collects information primarily from the employer about its employees. This information may be compared with information in several Federal databases both inside and outside of DHS.

**Employment Eligibility Information Collected from the E-Verify Employer**

Information about the employee to be verified

- All Employees
  - Name (last, first, middle initial, maiden)
  - Date of Birth
  - Social Security Number
  - Date of Hire: If date of verification is not within three days of hire date employer must select from a list of possible reasons why. Options include
    - Awaiting SSN
    - Technical Problems
    - Audit Revealed New Hire Was Not Run
    - Federal Contractor With E-Verify Clause Verifying Existing Employees
    - Other: If other is selected the employer will enter a free-text response
  - Claimed Citizenship Status
  - Type of Document Used for Acceptable Form I-9 Verification
  - Acceptable Form I-9 Document Expiration Date
  - Photographs, if required by secondary verification
  - Disposition data from the employer - the following codes are entered by the employer based what the employer does as a result of the employment verification information
    - *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;
    - *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;
    - *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;
    - *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;

- *The employee was terminated by the employer for receiving a Final Nonconfirmation 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 Tentative Nonconfirmation*: 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-USCs
  - A-Number
  - I-94 Number

<u>Information about the Employer or Designated Agent</u>

- Company Name
- Street Address (Post Office Boxes are not acceptable)
- Employer Identification Number
- North American Industry Classification System (NAICS) Code
- Number of Employees
- Number of Sites
- Parent Company or Corporate Company
- Name of Contact – Name of individual to be contacted for general issues regarding the company's participation in E-Verify
- Phone Number
- Fax Number

- 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
- User ID

**Employment Eligibility Information created by E-Verify**

E-Verify creates the following information based on an E-Verify query

- Case Verification Number
- VIS Response
    - Employment Authorized
    - SSA Tentative Nonconfirmation
    - DHS Tentative Nonconfirmation
    - 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 Final Nonconfirmation
    - DHS Verification in Process
    - DHS Employment Unauthorized
    - DHS No Show
    - DHS Final Nonconfirmation

**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 and compliance activities, including information placed in 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
- Information derived from telephone calls, emails, 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.

SSA's Numident System

- Confirmation of Employment Eligibility
- Tentative Nonconfirmation of Employment Eligibility and Justification
- Final Nonconfirmation of Employment Eligibility

USCIS's CIS

- Alien Number
- Last Name
- First Name
- Middle Name
- Date of Birth
- Date Entered United States
- Country of Birth
- Class of Admission
- File Control Office Code
- Social Security Number
- 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
- Naturalization Certificate Number
- EOIR Information, if in Proceedings

CBP NIIS and CBP BCI through the CBP TECS IT platform

- Alien Number
- Last Name
- First Name
- Maiden Name
- Date Alien's Status Changed
- Date of Birth
- Class of Admission Code
- Date Admitted Until
- Country of Citizenship
- Port of Entry
- Date Entered United States (arrival date)
- Departure Date
- I-94 Number
- Visa Number
- Passport Number
- Passport Information
- Passport Card Number

USCIS's ISRS

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

USCIS's CLAIMS 3

- Receipt Number
- Alien Number
- Last Name
- First Name

- Middle Name
- Address
- Social Security Number
- Date of Birth
- Country of Birth
- Class of Admission
- I-94 Number
- Employment Authorization Card Information
- Lawful Permanent Resident Card Information
- Date of Entry
- Valid To Date
- Petitioner Internal Revenue Service Number
- Attorney Name
- Attorney Address

ICE's SEVIS

- Student and Exchange Visitor Identification Number (SEVIS ID)
- Last Name
- First Name
- Middle Name
- Date of Birth
- Country of Birth
- Class of Admission
- I-94 Number
- Date of Entry
- Valid To Date
- Social Security Number
- Nationality
- Gender
- Student Status
- Visa Code
- Status Change Date
- Port of Entry Code
- Non Citizen Entry Date
- Status Code
- Program End Date

USCIS's CLAIMS 4

- Alien Number
- Social Security Number
- Last Name
- First Name
- Middle Name
- Birth Date
- Birth Country
- Nationality
- Gender
- Naturalization Verification (Citizenship Certificate Identification ID)
- Naturalization Verification (Citizenship Naturalization Date/Time)
- Address

USCIS's RNACS

- Alien Number
- Last Name
- First Name
- Middle Name
- Birth Date
- Birth Country
- Gender
- Nationality
- Naturalization Verification (Citizenship Naturalization Date/Time)
- Naturalization Verification (Citizenship Certificate Identification ID)
- Immigration Status (Immigration Status Code)
- Address

USCIS's AR-11

- Name
- Current Address
- Date of Birth
- Previous Address
- Alien Number
- Federal Bureau of Investigation Number
- Admission Number

- Previous Address

USCIS's CISCOR

- Receipt Number
- Beneficiary Alien Number
- Beneficiary Date of Birth
- Beneficiary Country of Birth
- Beneficiary Social Security Number
- Beneficiary Last Name
- Beneficiary First Name
- Beneficiary Middle Name
- Petitioner Alien Number
- Petitioner Social Security Number
- Petitioner Naturalization Certificate Number
- Petitioner First Name
- Petitioner Last Name
- Petitioner Firm Name
- Petitioner Tax Number

USCIS's NFTS

- Alien Number
- File Location

USCIS's MiDAS

- Name
- Alien Number
- Date of Birth
- Citizenship Number

USCIS's MFAS

- Individual's
    - Name (Last, First, Middle)
    - Date of Birth
    - Country of Birth
    - Country of Citizenship
    - Class of Admission
    - Date of Admission
    - Alien Number

  - Receipt Number
  - Phone Number
  - Marriage Date and Place
- Spouse's
  - Name (Last, First, Middle)
  - Date of Birth
  - Country of Birth
  - Country of Citizenship
  - Class of Admission
  - Date of Admission
  - Alien Number
  - Receipt Number
  - Phone Number
  - Marriage Date and Place
  - Naturalization Date and Place
- Children's
  - Names (Last, First, Middle)
  - Date of Birth
  - Country of Birth
  - Class of Admission
  - Alien Number
- Employer
  - Name
  - Address
  - Supervisor's Name
  - Supervisor's Phone Number

USCIS's EDMS

- All Information Contained in an Individual's A-File, including, but not limited to:
  - Alien Number
  - Last Name
  - First Name
  - Middle Name
  - Date of Birth
  - Date Entered United States
  - Country of Birth
  - Class of Admission
  - Social Security Number
  - Form I-94 Number
  - Naturalization Information and Certificate

- Photograph
- Marriage Information and Certificate

DOS's DOS-CCD

- Name
- Date of Birth
- Passport Number
- Visa Control Number
- FOIL Number
- Alien Number
- Photograph

ICE's EID Enforcement Alien Removal Module (EARM)

- Alien Number
- Name
- Marital Status
- Date of Birth
- Age
- Sex
- Country of Birth
- Country of Citizenship
- Date of Entry
- Class of Admission
- Social Security Number
- Federal Bureau of Investigation Number
- Case History
- Alerts
- Case Summary Comments
- Case Category
- Date of Encounter
- Encounter Information
- Custody Actions & Decisions
- Case Actions & Decisions
- Bonds
- Photograph

USCIS's RAPS

- Class of Admission
- Country of Birth
- Date of Birth
- Date of Entry
- Current Status
- Asylum Applicant Receipt Date

US-VISIT's ADIS

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

DOJ's EOIR

- Name
- File Number
- Address
- Nationality
- 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

## 1.2 What are the sources of the information in the system?

Information comes from employers, employer users, designated agents, employees, and from Federal government databases.

Employee seeking employment verification through E-Verify

Employees hired by employers participating in E-Verify submit certain biographical data elements to their employer using the Form I-9. The employer submits the information for verification through E-Verify.

Employer

Employers must provide certain company information as described in section 1.1 to participate in E-Verify. Employers may also provide information for purposes of licensing to use the E-Verify logo on their outreach materials.

Employer User

The employees who use E-Verify for the participating company provide limited identity information as described in section 1.1.

Designated Agents

Designated agents are required to enroll in E-Verify and be validated in the same manner as other participants. They will also submit information on behalf of the companies that have hired them to use E-Verify. Designated agents may also provide information for purposes of licensing to use the E-Verify logo on their outreach materials.

Federal Government Databases

E-Verify collects and uses information from the following systems:

- **Numident**: Numident is a Social Security Administration database containing the biographic information on all individuals who have received a social security card. E-Verify uses this information to verify whether an individual is employment eligible. This system is covered by the SORN for the SSA NUMIDENT System published January 11, 2006 at 71 FR 1796.

- **CIS:** CIS contains information on the status of 57 million applicants/petitioners seeking immigration benefits to include: lawful permanent residents, naturalized citizens, U.S. border crossers, aliens who illegally entered the U.S., aliens who have been issued employment eligibility documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA). Status Verifiers will use CIS as part of the secondary immigration status verification for E-Verify. The system is covered by the DHS/USCIS-001 CIS/A-File SORN published January 16, 2007 at 72 FR 1755.

- **SEVIS:** SEVIS maintains information on nonimmigrant students and exchange visitors (F, M and J Visas) and their dependents, and also on their associated schools and sponsors. SEVIS enables DHS

to maintain current information and facilitate oversight relating to nonimmigrant foreign students and exchange visitors during the course of their stay in the U.S. E-Verify is an existing user of the information from SEVIS and will use the information for primary verification of immigration status for E-Verify. Status Verifiers use SEVIS as part of the secondary immigration status verification for E-Verify. This system is covered by the DHS/ICE Student and Exchange Visitor Information System SORN published March 22, 2005 at 70 FR 14477.

- **CBP's NIIS and BCI :** CBP NIIS contains information obtained by DHS from I-94 and I-94W Forms presented by individuals entering or exiting the country and later entered manually... Border Crossing Information is the information collected from the individual at the time of the border entry from the documents presented to the CBP Officer, for example passports or visas. Status Verifiers will use this data as part of the secondary immigration status verification for E-Verify. These two collections are covered by the DHS/CBP-016 Nonimmigrant Information System (NIIS) published on December 19, 2008, at 73 FR 77739 and DHS/CBP Border Crossing Information (BCI) published July 25, 2008 73 FR 43457.

- **CLAIMS 3**: CLAIMS 3 is a mainframe database centered major application that supports processing of USCIS applications and petitions for various immigrant benefits (e.g. change of status, employment eligibility, extension of stay, etc). It supports case management for and adjudication of all USCIS benefits except naturalization and citizenship. Status Verifiers will use CLAIMS 3 as part of the secondary immigration status verification for E-Verify. This system is covered by the DOJ/INS Claims 3/Claims 4 SORN published March 13, 1997 62 FR 11919.

- **ISRS:** ISRS provides a searchable repository enabling access to digitized biometric information signatures, fingerprints, and photo images. ISRs contains biographic data and biometric image data including photographs, signatures, and fingerprints. Status Verifiers will use ISRS as part of the secondary immigration status verification for E-Verify. The system is covered by the DHS/USCIS--003 Biometric Storage System (BSS) SORN published April 6, 2007 at 72 FR 17172.

- **ADIS:** ADIS contains information on individuals arriving and departing at United States ports of entry. This information includes biographic information from passenger manifests and Forms I-94. E-Verify uses this information to verify an individual's eligibility to be in the country for employment purposes. Status Verifiers will use ADIS as part of the secondary immigration status verification for E-Verify. This system is covered by the DHS/US-VISIT-001 Arrival and Departure Information System (ADIS) SORN published August 22, 2007 at 72 FR 47057.

- **RNACS:** RNACS provides full case tracking and management capability for naturalization casework including assignment of cases to Case Control Offices (CCO); queuing of cases for appropriate actions, scheduling interviews and oath ceremonies; editing transactions; reporting; and

production of correspondence. E-Verify will use the information for primary verification of employment verification. This information will be used by VIS's automated online immigration status verification algorithm to determine if a person has a valid immigration status for employment. Status Verifiers will use RNACS as part of the secondary immigration status verification for E-Verify. This system is covered by a legacy JUSTICE/INS-031 SORN published April 29, 2002 at 67 FR 20996.

- **CLAIMS 4:** INS to provide immigration status verification information to help users determine eligibility for employment eligibility requests, and to assist in the processing of applications related to naturalization or attaining U. S. citizenship. Status Verifiers will use CLAIMS 4 as part of the secondary immigration status verification for E-Verify. This system is covered by the DOJ/INS Claims 3/Claims 4 SORN published March 13, 1997 at 62 FR 11919.

- **AR-11:** AR-11 collects and maintains immigrant and non-immigrant change of address records. AR-11 was established to maintain both immigrant and non-immigrant change of address records. Status Verifiers will use AR-11 as part of the secondary immigration status verification for E-Verify. This system is covered by the DHS/USCIS-001 CIS/A-File SORN published January 16, 2007, at 72 FR 1755.

- **CISCOR:** CISCOR is a consolidated repository and reporting data mart for data pulled from the Claims 3 LAN instances from the four USCIS Service Centers and the National Benefits Center. CISCOR consolidates the Claims 3 Local Area Network (LAN) data into a single repository, which is centrally managed. Status Verifiers will use CISCOR as part of the secondary immigration status verification for E-Verify. The system is covered by the DHS/USCIS-001 CIS/A-File SORN published January 16, 2007 at 72 FR 1755.

- **NFTS:** NFTS provides a centralized, automated, mechanism for determining the location of a physical A-File and associated Receipt Files. NFTS supports the Records requirement to track files at the local level, as well as the national level. It is designed to support the Records mission and to provide efficient access to high-quality immigrant information by maintaining an accurate file inventory. Status Verifiers will use NFTS as part of the secondary immigration status verification for the E-Verify program. This system is covered by the DHS/USCIS-001 CIS/A-File SORN published January 16, 2007 at 72 FR 1755.

- **MiDAS:** MiDAS is an image-based search and retrieval application of digitized alien records on individuals who entered the U.S. between 1906 and 1975 (50-60 million records). MiDAS allows USCIS Office of Records to achieve a more effective search result and improved customer service. When digitization of all files is complete, the MiDAS database will hold over 80 million records including Master Index, Flex-O-Line, A-files, Citizenship/Naturalization files (C-files, 129, 3904, OM, etc), file locator information cards, and other historical records. Status Verifiers will use

MiDAS as part of the secondary immigration status verification for E-Verify. This system is covered by the legacy JUSTICE/INS –001 INS Index System SORN, published in 1993 at 58 FR 51847.

- **MFAS:** The Marriage Fraud Amendment System (MFAS) supports and maintains casework resulting from the Immigration Marriage Fraud Amendment Act (MFA), which became law on November 10, 1986. MFAS allows users the ability to process and control applications and petitions to grant Conditional Permanent Resident (CPR) status and Permanent Resident (PR) status, and to identify and terminate the CPR status of aliens who acquired this status fraudulently or who have not removed this status during the designated time-period that the law requires. Status Verifiers will use MFAS as part of the secondary immigration status verification for the E-Verify program. While the data from MFAS will be used for verification it will not be stored in VIS. This system is covered by the DHS/USCIS 007 USCIS Benefits Information System SORN, published September 9, 2008 at 73 FR 56596.

- **EDMS:** The Enterprise Document Management System (EDMS) is a web-based system that allows users to view, search, and add comments to digitized alien files (A-Files). Status Verifiers will use EDMS when required to access an A-File as part of the secondary verification process. While the data from EDMS will be used for verification it will not be stored in VIS. This system is covered by the DHS/USCIS-001 CIS/A-File SORN published January 16, 2007 at 72 FR 1755.

- **Department of State Consular Consolidated Database (CCD):** Consular personnel use CCD as a resource for verifying prior visa issuances/refusals and for statistical reporting. Status Verifiers will use DOS-CCD as part of the secondary immigration status verification for the E-Verify program. While the data from DOS-CCD will be used for verification, it will not be stored in VIS. This system is covered by the Department of State Visa Records STATE-39 SORN, which can be found on the Department of State website (http://foia.state.gov/issuances/STATE-39.pdf).

- **EID EARM:** EID contains biographic and case information on aliens encountered and booked in Immigration and Customs Enforcement (ICE) and other DHS component enforcement actions. Status Verifiers will use EID as part of the secondary immigration status verification for the E-Verify program. Information from EID is required by the Status Verifiers in order to help determine whether an individual may not be eligible for employment, government benefit, credential, or other reason for which they are having their immigration status verified in the first place. DHS components collect the information in EID during enforcement or administrative actions. Its use for verification of immigration status follows because in all cases that the verification is performed, eligibility may be contingent on not having been the subject of an enforcement action. This system is covered by the DHS/ICE-011 Immigration Enforcement Operational Records (ENFORCE) SORN published March 1, 2010, at 75 FR 74729.

- **RAPS:** RAPS contains biographic information collected for USCIS Form I-589, Asylum Application. Status Verifiers use RAPS as part of the secondary immigration status verification for E-Verify. Information from RAPS is required by the Status Verifiers in order to help determine whether an individual is ineligible for employment. DHS components collect the information in RAPS when an applicant for asylum completes a Form I-589. Its use for verification of immigration status follows because asylum brings with it access to certain benefits. It is essential to ensure that individuals are appropriately seeking verification for purposes of gaining employment. This system will be covered by the RAPS SORN when published.

- **EOIR:** This Department of Justice system contains information pertaining to aliens and alleged aliens brought into the immigration hearing process, including certain aliens previously or subsequently admitted for lawful permanent residence. Status Verifiers will use EOIR as part of the secondary immigration status verification for the E-Verify program when there is a question of immigration status. Information from EOIR is required by the Status Verifiers in order to help determine whether an individual may not be eligible for employment, credential, or other reason for which they are having their immigration status verified in the first place. Its use for verification of immigration status follows because in all cases that the verification is performed, eligibility may be contingent on not having been the subject of an enforcement action. This system is covered by the Justice/EOIR-Records and Management Information System SORN published October 10, 1995, at 60 FR 52690 and updated July 5, 2001 at 66 FR 35458.

- **Compliance Tracking and Management System (CTMS):** This USCIS system supports E-Verify monitoring and compliance activities. This information may be used to prevent misuse of the E-Verify Program. This system is covered by the Compliance Tracking and Monitoring System (CTMS) SORN published May 22, 2009 at 74 FR 33825.

## 1.3 Why is the information being collected, used, disseminated, or maintained?

E-Verify collects information from an employer in order to register the employer in E-Verify. E-Verify collects personally identifiable information from individual users of the system in order to provide accountability of system usage in the event a problem arises with misuse of the system or to contact users in the case of a system-related issue that needs to be reported to the users.

E-Verify collects information from employees for identification and employment eligibility verification.

E-Verify also collects information from the press and general public who are interested in receiving information and outreach contacts on the E-Verify program. E-Verify collects

information from individuals who contact USCIS to report a problem or potential problem with the use of E-Verify through the call center.

As discussed in the Person Centric Query (PCQ) Service PIA Update, the addition of the PCQ Service for Status Verifiers will identify inconsistencies between databases, which should reduce the time it takes to identify and resolve TNCs. E-Verify has added the Photo Screening Tool, which presents a photo to the employer using E-Verify. This will allow the employer and DHS to identify possible identity fraud. It does not allow the employer to retain the photo provided by the system. E-Verify also collects information in the course of its monitoring and compliance activities, especially in connection with determining the existence of fraud or discrimination in the use of the E-Verify system. This information is maintained in the CTMS system.

## 1.4 How is the information collected?

E-Verify collects the initial information entered by the employer or designated agent into E-Verify based on the information the employee provided on their Form I-9. Information may also be collected when an individual contacts E-Verify or E-Verify contacts users or employees for general program or issue specific purposes such a satisfaction surveys or system outage notifications.

E-Verify may be accessed through various secure means to include: 1) Secure File Transfer Protocols for batch transfers, 2) dial up systems (currently being phased out), 3) secure USCIS web site, or 4) web services that allow direct connection between USCIS and the employer. Once the information is collected an automatic verification process is conducted against a limited number of Federal databases including SSA Numident and DHS CIS and TECS. If the information is verified, then no further collection is required. If the information cannot be verified, then the employee will be given the option to submit additional verifiable information or to correct information previously received. Status Verifiers may check additional systems to verify this information.

E-Verify also collects information in the course of its monitoring and compliance activities from VIS and emails, telephone calls, letters, desk audits, and site visits. Information will be collected from tips of a prohibited behavior from the Verification Call Center, law enforcement agencies, and the media. The information collected from the Call Center will be collected as part of the Call Center normal activity of collecting information from callers.

E-Verify may also collect contact information from individuals, businesses, or organizations who request to be contacted by E-Verify for general program or issue specific information.

## 1.5 How will the information be checked for accuracy?

With respect to information collected for verifications, it is incumbent upon the individual being verified as well as the Employer User performing the query to verify the accuracy of information that is entered into E-Verify. E-Verify displays a confirmation page to the Employer User and Designated Agent to review the employee's information prior to submitting the query.

In response to an initial verification query on an employee, E-Verify will provide either the Employment Authorized result or an indication that the information provided by the employee does not match the information in the SSA or DHS databases. The employee has the option to contest and will contact either SSA or DHS as appropriate to resolve the problem.

The Status Verifier will search other data sources to produce definitive results. Once the Status Verifier has resolved the problem, they will update E-Verify to reflect an Employment Authorized result for the employee and when possible will request an update to the underlying database.

One of the fundamental purposes of monitoring and compliance is to review the information to determine whether it is accurate and in doing so, whether the information will indicate whether a non-compliant behavior has occurred. The information collected into CTMS from VIS is verified by comparing it with the actual information submitted for the original verification. In addition, by interviewing users and verification subjects and collecting employment and other business records, USCIS can determine if there are inconsistencies in the information.

## 1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), P.L. 104-208, dated September 30, 1996

The IIRIRA required a means to respond to inquiries by federal, state, and local benefit issuing agencies and institutions seeking to verify or determine the citizenship or immigration status of any individual within the jurisdiction of the Agency for any lawful purpose. Title IV of the Act requires the establishment of a Basic Pilot Program with voluntary participation by employers who could use this system to determine whether newly hired employees are authorized to work in the United States.

Basic Pilot Program Extension and Expansion Act of 2003 (Pub. Law 108-156), dated November 19, 2003

This Act extended the Basic Pilot to November 2008.

Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 PL 110-329, dated September 30, 2008

Congress passed the Department of Homeland Security's fiscal year 2009 appropriation legislation that was signed into law, and provided $100 million to continue, expand and improve E-Verify in fiscal year 2009.

### 1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There were two privacy risks identified – the risk of collection of extraneous information and the risk of inaccurate information attributed to the individual. Limiting the collection of information mitigates the risk of collection of extraneous information. E-Verify collects only that personally identifiable information on the employee needed to verify employment eligibility. The use of multiple databases to confirm the information mitigates the risk of inaccurate information attributed to the individual. E-Verify includes data from numerous Federal government databases to improve the completeness and accuracy of data within E-Verify. Additionally, if E-Verify is unable to automatically verify an individual's status in order to authorize employment, a Status Verifier will review the information and conduct searches of other Federal government databases.

With respect to monitoring and compliance activities, CTMS will consist of information authorized for the protection of the integrity of E-Verify, and to prevent fraud and discrimination in connection with the use of the E-Verify system, including protection of individual rights, civil liberties, and privacy. The information collected and used in CTMS will be the minimal amount of information needed to confirm or disprove an identified or suspected occurrence of a prohibited behavior. The amount of information collected cannot always be identified before research begins; however, the monitoring and compliance activities are being defined in standard operating procedures (SOPs) that include procedures to limit the collection of information to only the information required.

## Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

## 2.1 Describe all the uses of information.

Employers use E-Verify to determine whether a newly hired employee is authorized to work in this country based on the existence of a valid Social Security Number and lawful immigration status. The employer collects this information from the employee, entered into E-Verify, and compared against information contained in Federal government databases. In addition, when an employee presents certain employment documents, E-Verify will allow employers to view digital photographs from selected Federal government databases in order to assist the employer with another means of verifying an employee's identity. If there appears to be evidence of document fraud, the employer is instructed to notify USCIS.

Additionally, the information in E-Verify may be used for the following purposes: 1) law enforcement to prevent fraud and misuse of E-Verify, and to prevent discrimination and employment-based identity theft; 2) program management; 3) data analysis; 4) monitoring and compliance, including information placed in CTMS; 5) program outreach; and 6) prevention of fraud and discrimination. On a case-by-case basis, E-Verify may give law enforcement agencies extracts of information on potential fraud, discrimination or other illegal activities. E-Verify will use information in the system for program analysis to improve the operation of the program and to enhance its capabilities. This type of use may include conducting surveys and using information for system development and testing purposes. E-Verify will use information in the system to ensure that users are complying with program requirements and defined procedures. E-Verify will use information in the system for program outreach such as to ensure users are receiving assistance as necessary. Designated agents also may use program outreach materials such as E-Verify information and logo if they have agreed to certain licensing restrictions.

## 2.2 What types of tools are used to analyze data and what type of data may be produced?

E-Verify will use both manual and automated comparisons of information to confirm identity and employment eligibility. E- Verify has audit and reporting capabilities to better assist E-Verify in identifying misuse of the system. For purposes of monitoring and compliance, data is analyzed to identify misuse, abuse, discrimination, breach of privacy, and fraudulent use of the E-Verify system. This consists of searching for pre-defined patterns and data irregularities and applying thresholds, where applicable, against this data, which may indicate that a particular non-compliant behavior has occurred. For example, E-Verify will focus on whether the system is being used in a discriminatory fashion, i.e., used to verify some employees but not others, as well as whether the system is used to prescreen employees as opposed to being utilized after an offer of employment has been extended.

E-Verify creates the following information based on an E-Verify query:

- Case Verification Number
- VIS Response
  - Employment Authorized
  - SSA Tentative Nonconfirmation
  - DHS Tentative Nonconfirmation
  - SSA Case in Continuance
  - DHS Case in Continuance
  - SSA Final Nonconfirmation
  - DHS Verification in Process
  - DHS Employment Unauthorized
  - DHS No Show
  - DHS Final Nonconfirmation

## 2.3 If the system uses commercial or publicly available data please explain why and how it is used.

E-Verify does not use commercial or publicly available data.

## 2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The information contained in E-Verify is used primarily to respond to employment verification inquiries from authorized employers. Employers must sign a MOU with DHS stating the intended use of the system and agreeing to the established security requirements. Each MOU contains provisions for training, policies, safeguarding of information obtained from the system, and procedures/instructions on the use of E-Verify. There are three privacy risks associated with the use of E-Verify information: information misuse, unauthorized access to information, and inaccurate attribution of information. Because E-Verify collects and uses a significant amount of personal information it may be misused by the employer users, designated agents, or DHS. Employers must sign MOUs and successfully complete training to ensure that they understand the proper use and handling of E-Verify information. The legal authorization for E- Verify strictly limits the uses to which E-Verify information may be put. Furthermore, E-Verify has audit and reporting capabilities to assist in identifying misused information.

The second risk is that individuals without authorization may gain access to E-Verify information. Currently, E-Verify conducts only rudimentary validation of employer's identities when they enroll with E-Verify. This could potentially result in individuals impersonating a legitimate employer and using the system to validate information for identity theft purposes. In order to mitigate this risk, E-Verify is currently working to establish a process for validating the

identity of employers. Once an employer enrolls with E-Verify, they are required to sign an MOU agreeing to appropriate safeguards, use, maintenance, and disclosure of the data. This includes the use of logins and passwords to limit access to E-Verify to only those individuals who have a need to access the system and who have completed the training.

The third risk is that inaccurate information may be attributed to an individual. Information in E-Verify comes from various sources including direct entry into the system by employer users and designated agents and also from numerous DHS federal databases. Having multiple data sources means that it is more likely that at least one of the sources has data inaccuracies or misattributions of information. E-Verify attempts to overcome this risk by comparing several Federal government databases using both automated and manual procedures. The Status Verification procedures for conducting manual searches and updating any underlying information contained within the various DHS databases improves the accuracy of the information in E-Verify overall.

# Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

## 3.1 What information is retained?

E-Verify will retain all of the information collected from the employer, employee, and some of the information collected from the various Federal government databases used to verify or correct the information received from the employer or employee. In addition, E-Verify will retain all information created by the E-Verify Program, including the employment eligibility status. E-Verify does not retain the passport or visa photo provided by the Department of State for the photo tool verification. In the processes of resolving a TNC, an employee may provide to E-Verify Status Verifiers hard copies of their identification documents or government forms that demonstrate identity or employment eligibility. The vast majority of these hard copies are retained only for the period necessary to resolve the TNC and are then destroyed. Some hard copies of verified fraudulent documents may be retained for training purposes.

## 3.2 How long is information retained?

E-Verify will retain information for ten (10) years from the date of the completion of the verification, 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).

### 3.3 Has the retention schedule been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention schedule N1-566-08-7 has been approved by NARA as of June 5, 2008.

### 3.4 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

All E-Verify information is retained for a period of ten (10) years to coincide with 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). While the business justification for this retention is clear—pursuing E-Verify fraud or misuse cases—the primary privacy risk associated with retaining the information for ten years is that the information might be misused. This risk is mitigated by policy and technical controls that limit use and access to E-Verify information. By policy, this information may only be used for the employment eligibility purpose of the E-Verify Program or for purposes that directly support the program such as prevention of misuse and fraud, program analysis, and outreach. Furthermore, the information in VIS the underlying technology solution for E-Verify, is purely transactional and individuals with access to the system have procedural and technical limitations that prevent them from searching the database for such things as work history or even previous E-Verify verifications. The E-Verify Program has also developed compliance and monitoring capabilities to detect and minimize potential misuse of the E-Verify information.

## Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

### 4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

When potential fraud or misuse is indicated by E-Verify information, this information may be shared, on a case-by-case basis, with DHS internal law enforcement organizations such as the Immigration and Customs Enforcement (ICE). For example, information could be shared with ICE if it was discovered that a SSN was used repeatedly in ways that were inconsistent with one legal

worker using his own SSN. In these cases, E-Verify will share only that information required to pursue an investigation into the potential fraud or misuse.

### 4.2 How is the information transmitted or disclosed?

Information on either a discrete transaction or information on a large number of transactions may be extracted and securely shared with ICE. Any data sharing will be conducted in accordance with all existing sharing procedures to ensure that appropriate DHS security and privacy requirements are met. In most cases, this would mean that information would be electronically extracted from VIS, as the E-Verify underlying technology, and securely transmitted over the DHS secure local area network to the responsible law enforcement officer working the potential case. The extraction would be required to comply with all DHS and Federal requirements including the Office of Management and Budget (OMB) Memorandum 06-16.

### 4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

E-Verify will only share information internally for law enforcement purposes regarding potential fraud or misuse of E-Verify. USCIS will use existing sharing policies and procedures to ensure that appropriate protections are used. In addition, all DHS employees are also required to take and pass annual computer and privacy awareness training that addresses the handling of shared personal information.

## Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS which includes Federal, state and local government, and the private sector.

### 5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

As part of the normal E-Verify business process certain information collected from the employee or employer may be submitted to external organizations for verification purposes and in the reverse, certain information is returned to the E-Verify employer and employee. E-Verify information including the employee's name, SSN, and date of birth is submitted to the Social Security Administration for SSN verification. The Social Security Administration retains this information for auditing purposes in accordance with the Numident retention schedule. E-Verify returns employment eligibility status information to the employer indicating whether an employee is employment authorized or whether the employee needs to take some action to

resolve a discrepancy in their records. The information that is returned is very limited. If the employee needs to take some action to correct their records, the details of the problem are not provided, rather the employee is told how to contact the correct agency—DHS or SSA—to resolve the discrepancy.

Under certain circumstances, such as when an employee uses an Employment Authorization Document or a Permanent Resident Card for their E-Verify document requirements, E-Verify will share a copy of the photo on record to the employer. The employer is required to compare the picture on the document offered by the employee with the picture presented by E-Verify. The photo is not retained on the employer's computer and is available only for document verification purposes.

In addition, E-Verify is currently developing the capability to verify employer information. This will ensure that all companies are legitimate and have the authority to conduct E-Verify queries. This process has not been finalized so it will be described more fully in a future PIA.

Finally, E-Verify information may also be shared with external law enforcement agencies, such as the Department of Justice, Civil Rights Division, when the information could be used to assist in investigations of discrimination, fraud, or other misuse of E-Verify.

## 5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

The primary external sharing that takes place is part of the normal business process of E-Verify where information submitted by employers and employees is submitted for verification to some external organizations and the verification results are shared back to the employers and employees. These instances of sharing are fully consistent with the purpose as described in the Purpose Section of the E-Verify SORN. External sharing for law enforcement purposes to assist in the investigations of fraud, misuse, and discrimination cases related to employment is fully within the purpose of the original collection and supported by routine uses section H and K of the SORN.

## 5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

E-Verify information shared with the employers and employees is provided over secure Internet connections between the employer and E-Verify. This may be through the E-Verify Web site or the employer may develop a web services tool to directly and securely connect with VIS. In either case, before the employer is given access to run E-Verify queries they are required to sign a MOU, which includes specific security requirements that they must comply with in the handling of E-Verify information. They are also required to take E-Verify training, which includes information on security and privacy.

E-Verify information shared with other Federal government databases, such as Numident, during the normal business process of employment verification are shared over secure lines to prevent unauthorized access. An MOU limits the use to the verification of the information.

E-Verify information shared for purposes of law enforcement is on an ad hoc basis to respond to an indication of a potential case to prevent fraud and misuse of E-Verify, and to prevent discrimination and employment-based identity theft based on E-Verify. The method of sharing and protections involved in that sharing will depend on the particular case. For example, the information that indicates that a single SSN has been used hundreds or thousands of times all over the United States in a short period of time may require an electronic extraction of information that will be protected with encryption and securely transmitted to the responsible law enforcement officer working the potential case. The extraction would be required to comply with all DHS and Federal requirements including the Office of Management and Budget (OMB) Memorandum 06-16. Alternatively, a single E-Verify transaction that appears to indicate fraud or misuse may be extracted in hardcopy and delivered directly to the responsible law enforcement officer working the potential case or extracted, encrypted, and transmitted to an external law enforcement entity.

## 5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Currently, the E-Verify Program has identified two (2) primary risks associated with external sharing of E-Verify information, the risk of unauthorized access and the risk of misuse by authorized users. E-Verify currently does not verify that a company that signs up to use E-Verify is actually an employer. This could result in individuals or groups posing as legitimate employers being able to run E-Verify queries and potentially validating that certain identifying information is correct. This could then be used for identity theft purposes. E-Verify is currently working on a procedure to verify the identity of employers. More information on this mitigation will be provided in an upcoming update to this PIA when this process is closer to maturity. In the mean

time, the E-Verify Program has developed monitoring and compliance capabilities that can be used to identify when this risk is indicated.

The risk of unauthorized access is also mitigated by having secure means for sharing information. This minimizes the chance of unauthorized access of the shared information.

The second risk regarding the external sharing of E-Verify information is that an authorized user may misuse the information provided. For example, it is possible that an employer who receives a TNC on an employee would release that employee because of the TNC. This is a misuse of the system that deprives the employee of their right to work and could constitute illegal activity on the part of the employer. In most cases these types of misuse are probably based on the employer not understanding his obligations and responsibilities for participating in E-Verify. E-Verify is attempting to mitigate this risk through additional training and outreach, as well as using the monitoring and compliance capabilities to identify potential cases of misuse, and to focus compliance assistance activities and share with OSC or other law enforcement agencies if appropriate.

# Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

## 6.1 Was notice provided to the individual prior to collection of information?

E-Verify requires employers to display informational posters notifying all employees that the employer is participating in E-Verify. These posters provide information on the employee's rights and on what they can do to enforce those rights. Employers may also use the E-Verify logo if they have agreed to the licensing restrictions. In addition, the Form I-9 instructions provide additional information about the purpose of the collection and use of the employee's information. E-Verify also provides outreach through a website and public advertising. Notice is provided by means of this PIA and the accompanying SORN which is being published concurrently with this PIA, which inform individuals that the Verification Division will collect and use information for certain purposes including those associated with preventing misuse, abuse, discrimination, breach of privacy, and fraudulent use of E-Verify information and systems.

## 6.2 Do individuals have the opportunity and/or right to decline to provide information?

In most cases, participation in E-Verify is voluntary for employers, but if an employer chooses to participate, all newly hired employees must be verified. If an employee refuses to provide the required information, the participating employer may terminate that employee. In some cases E-Verify is mandatory, either for geographic areas, such as the state of Arizona, or for certain jobs, such as federal employment. In these cases an employee has no real option to look for alternative employment that does not require verification. There is no ability to minimize this privacy risk and this must be accepted as a realized privacy issue that the Federal government is willing to accept based on the inevitable result of passage of laws that make participation in E-Verify mandatory.

## 6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

E-Verify verifies the employment eligibility of individuals who are working for participating employers. An employee's information is used solely to ascertain whether or not an individual is employment authorized. The employee is given notice at the time of employment that an employer is participating in E-Verify. Failure to provide consent to the use of their information for verification purposes by completing the Form I-9 may result in termination of employment.

## 6.4 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

There are two (2) privacy risks associated with notice and consent: 1) an employee may not have sufficient notice of the collection and use of their information, and 2) an employee does not have a real opportunity to consent to the collection and use of their information. Notice is provided in a number of ways including:

- requiring that posters be displayed prominently by the E-Verify employers,
- providing a Privacy Act notice in the Form I-9 instructions that describe the collection and use of the employee's information,
- providing outreach such as an E-Verify website with information on the employee's rights and options, and
- by means of this PIA and accompanying SORN.

Where E-Verify is mandatory, an employee may have no real opportunity to consent to the collection or use of their information. While employees may not be obligated to work for a particular employer, if all employers in their field or in their geographic location are E-Verify participants, then the employees have no real opportunity to consent. There is no way to minimize this privacy risk and therefore it must be accepted as a realized privacy issue that the Federal government is willing to accept based on it being the inevitable result of making E-Verify mandatory.

# Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

## 7.1 What are the procedures that allow individuals to gain access to their information?

Individuals may request access to their information by submitting a Privacy Act request to USCIS in writing clearly marked "Privacy Act Request" at the following addresses:

National Records Center
FOIA/PA Office
P.O. Box 648010
Lee's Summit, MO 64064-8010

Requesters are required to provide their full name, date, and place of birth, and return address. USCIS uses this information to identify relevant records and to verify the identity of the requestor.

## 7.2 What are the procedures for correcting inaccurate or erroneous information?

There are two ways to correct incorrect information. Inaccuracies identified during the E-Verify process will result in an employee receiving a TNC. The employee may resolve these types of inaccuracies through the standard verification process. They will be directed to contact either DHS or SSA depending on the type of inaccuracy. They may be required to provide additional information to correct the inaccuracy.

Inaccuracies may also be corrected through the FOIA/Privacy Act redress request process. The individual seeking redress would contact the FOIA/PA Officer at the address provided in Section 7.1, and provide them with the information necessary to correct their information.

### 7.3 How are individuals notified of the procedures for correcting their information?

When an employee contests a TNC, the employer provides information from E-Verify on how to contact SSA or DHS, as appropriate. The FOIA and Privacy Act Redress process is detailed on the E-Verify website and in this PIA.

### 7.4 If no formal redress is provided, what alternatives are available to the individual?

Formal redress is provided.

### 7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

E-Verify mitigates the risk that individuals will not have the opportunity to access and correct their personal information by providing two layers of correction and redress. During the verification process an employee may take steps to correct their information if they receive a TNC. Corrections are made by SSA or DHS. After the verification process is complete, individuals have the opportunity to access and correct their information through the FOIA/PA process.

There is a risk that an employer may not provide the information required for an employee to correct the information that resulted in a TNC. The E-Verify Program has mitigated this risk developing monitoring and compliance capabilities which can identity and minimize this risk.

## Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

### 8.1 What procedures are in place to determine which users may access the system and are they documented?

E-Verify has documented procedures for providing system access to both external users—employer participants and DAs—and internal users—certain USCIS employees. Externally, E-Verify allows the following types of authorized Users to submit E-Verify queries:

- General User: This user type performs verification queries, views reports, and has the capability to update their personal user account. Additionally, they have access to any open and closed cases that they initiated.

- 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 (including queries performed by other Users), perform queries, update account information, and unlock user accounts.
- Corporate Administrator: This user type can view reports for all companies associated with the E-Verify corporate account. 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.

Before employers may access E-Verify, they must sign a binding MOU regarding appropriate system use. In addition, E-Verify requires employers to complete a web-based training course that explains functionality and security requirements.

E-Verify allows the following types of internal users:

- Administrators: This user type is responsible for creating user accounts and administering the system. They can view reports, create and update account information, and unlock user accounts.
- Status Verifiers: This user type is responsible for assisting employees in resolving TNCs and performing analysis on system data. They can run queries, perform analysis, and manage their personal accounts.
- Managers: This user type is responsible for managing the actions that the Status Verifier takes when using E-Verify. They can assign and manage workloads and correct Status Verifier work.
- Analyst: This user type is responsible for reviewing data, including transaction records, hotline calls, and external information and audit logs.
- Auditor: This user type is responsible for reviewing audit logs to ensure that users are correctly and appropriately using the system.

All internal access to E-Verify is based on user accounts and passwords that are issued to individuals who have the authority and business need to access E-Verify. Access is granted following DHS policies and procedures.

## 8.2 Will Department contractors have access to the system?

Yes, contractors will have access to E-Verify.

## 8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

Internal users of E-Verify take mandatory, annual DHS Information Technology security and privacy awareness training.

External users of E-Verify are provided an on-line tutorial that includes privacy and security training for the E-Verify Program.

## 8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes. VIS as the underlying technology supporting E-Verify has been Certified and Accredited and received a full authority to operate in April 2008. This accreditation expires April 2011, or before if significant changes are made to VIS.

## 8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

E-Verify has implemented a broad range of technical, operational, and physical security measures to protect the system and its information. These security measures include access controls for both internal and external users. For example, account names and passwords are required to access E-Verify. E-Verify has an automated mechanism to ensure that users change their passwords at a specified interval. User accounts are locked after several failed attempts to log on. E-Verify protects against password re-use. Additionally, inactive E-Verify sessions will timeout, requiring the user to log in again. Other examples of security controls include:

- Password data is encrypted within the system
- E-Verify is located within a multi-layered firewall architecture
- A robust set of security controls that meet DHS System Security Policy requirements are documented and verified through the certification and accreditation process
- E-Verify uses HTTPS protected communications during all data transmissions between the client workstation and the system
- VIS passwords are encrypted when making database connections
- Procedures are in place to ensure that any potential breaches of information are reported within one hour of being found

E-Verify has a comprehensive audit trail tracking and maintenance function that stores information on users who submit queries, when the query was processed, what the response was, who receives the response, and when the response was received. The audit logs have restricted access based on user roles. These logs are external to system administration access methods and protected from modification. These audit logs are periodically reviewed for monitoring user activity. Employer users are required to abide by all security requirements as agreed to when they enrolled in E-Verify. Attempts to evade the security controls can result in loss of access to E-Verify.

### 8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Because of the sensitivity of the information collected and used by E-Verify an extensive set of technical, operational, and physical security controls have been implemented to protect this information. These controls meet or exceed the DHS and Federal requirements as described in the DHS Sensitive System Policy and Handbook and various OMB Memoranda.

Specifically, the risk of unauthorized users gaining access to E-Verify is mitigated through various access controls including user accounts, complex passwords that must be changed often, active session timeouts, and auditing of system use. The risk of authorized users misusing the system is mitigated through auditing and monitoring capabilities that are sufficiently detailed to hold users accountable for their actions when using E-Verify.

## Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

### 9.1 What type of project is the program or system?

E-Verify is comprised of an underlying technical infrastructure and operational policies and procedures for the verification of employment authority. VIS, as the underlying technology, is composed of database and web servers, and communication and security infrastructure.

### 9.2 What stage of development is the system in and what project development lifecycle was used?

E-Verify is in the Operations and Maintenance Stage of the DHS Lifecycle Development Process.

### 9.3 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

E-Verify is primarily an electronic database that can be accessed—externally over the Internet and internally over the secure DHS intranet—by E-Verify users. The risks and mitigations associated with this privacy sensitive technology are discussed throughout this PIA.

## Responsible Officials

Claire Stapleton, Chief
Privacy Branch, Verification Division
United State Citizenship and Immigration Services
Department of Homeland Security

## Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security